A Framework for Misuse Detection in Ad Hoc Networks–Part I

Dhanant Subhadrabandhu, Saswati Sarkar and Farooq Anjum

Abstract— **We consider ad hoc networks with multiple, mobile intruders. We investigate the placement of the intrusion detection modules for misuse based detection strategy. Our goal is to maximize the detection rate subject to limited availability of communication and computational resources. We mathematically formulate this problem, and show that computing the optimal solution is NP-hard. Thereafter, we propose two approximation algorithms that approximate the optimal solution within a constant factor, and prove that they attain the best possible approximation ratios. The approximation algorithms though require re-computation every time the topology changes. Thereafter we modify these algorithms to adapt seamlessly to topological changes. We obtain analytical expressions to quantify the resource consumption versus detection rate tradeoffs for different algorithms. Using analysis and simulation we evaluate these algorithms, and identify the appropriate algorithms for different detection rate and resource consumption tradeoffs.**

Index Terms— **Ad hoc networks, distributed algorithm, optimization, resource management, site security monitoring.**

I. Introduction

Ad hoc networks provide the only means of electronic communication in areas where establishing infrastructure like base stations is either impossible or not cost-effective. Examples include disaster recovery operations, battlefields, communication in remote terrains (e.g., reservations, rural areas), events like superbowl matches, etc. These networks are used by a diverse user population, e.g., civilians in disaster hit areas, spectators in superbowl matches etc., which increases the security risks. One such risk is a user who subverts the functioning of the network by causing undesirable events. Such users are considered as intruders and the events as intrusions. Examples of intrusions are attacks such as TCP SYN flood*, Land Exploit†, SSPing‡ etc. [6], [7]. These intrusions leverage system vulnerabilities. There are two ways to prevent such intrusions. One way is to remove the vulnerabilities from the system such as by designing resistant protocols like SCTP [23] to resist TCP SYN flood attacks, patching the operating systems, etc. But, this may not be possible due to various reasons such as poor design [17], limited use of efficient technical solutions (e.g., SCTP is rarely used due to large scale deployment of TCP), different devices having different capabilities, inefficient configuration (e.g., users do not change default security settings or apply patches), etc. The second approach, which is complimentary to the first, is to detect attempts to leverage the vulnerabilities and stop such attempts from succeeding. We focus on the detection aspect of the second approach. We refer to this as intrusion detection.

Intrusion detection has been extensively investigated for wireline networks [8], [9]. But techniques geared towards wireline networks would not suffice in an ad hoc network due to mobility, the ease of listening to wireless transmissions, lack of fixed infrastructure, etc. [11]. For example, several detection strategies in wireline networks are based on the presence of a small number of static gateways that route and therefore monitor all traffic. But, ad hoc networks typically do not have such choke points, and if such choke-points exist, their locations continuously change due to mobility. Also, intrusion may be detected in wireline networks by detecting anomaly, i.e., by comparing the current system behavior with that in absence of intrusion. In ad hoc networks, however, normal behavior can not be accurately characterized, e.g., a node may transmit false updates since the routing protocol is slow to converge and not because it is malicious. Further, unlike in wireline networks, nodes in an ad hoc network have limited energy. Hence, only computationally simple, energy-efficient detection strategies can be used. The detection algorithms must also be distributed as communication with a central computing unit will consume significant energy and bandwidth. Finally, the detection algorithms must seamlessly adapt to topological changes due to mobility. These motivate the design of detection strategies specifically geared towards ad hoc networks.

A strategy specifically suitable for ad hoc networks is that of misuse detection that relies on the use of known patterns of unauthorized behavior. This technique detects intrusion when the transmitted traffic contains abnormal packets which serve as "signatures" of attacks. For example, a UDP packet destined to port 0 can crash some machines [7]. The signature of ping-of-death attack is a very large ping packet, that of RPC locator attack is a packet intended for port 135 that contains a command that the system is not expecting, that of Bubonic attack are various values such as time-to-live (TTL) of 255, type-of-service (TOS) field value of $0xC9$, exactly 20 byte payload in the IP datagram and the fragment ID value with consistent increments of 256 [7]. Due to low false alarm rates, misuse detection is the mainstay of current commercial intrusion detection systems in wireline networks and wireless local area networks. This technique can not however detect new attacks, i.e., the attacks whose signatures are unknown. Nevertheless, it is the most suitable technique in ad hoc

D. Subhadrabandhu and S. Sarkar are at the department of Electrical and Systems Engineering at the University of Pennsylvania. F. Anjum is at the Telcordia Technologies. Their emails are dhanant@seas.upenn.edu, swati@seas.upenn.edu, and fanjum@telcordia.com. The contribution of S. Sarkar was in part supported by the National Science Foundation under grants ANI-0106984, NCR-0238340 and CNS-0435306.

*The attacker opens a large number of half-open TCP connections.

†The attacker sends a TCP SYN packet with the same target and source address.

‡The attacker sends a series of fragmented, oversized ICMP packets.

networks given that it does not require characterization of normal behavior.

But a prerequisite for deploying misuse detection in ad hoc networks is to determine which nodes should execute the sniffing and analysis software modules which we refer to as the intrusion detection system (IDS) modules. We show that different selection strategies can have significantly different detection efficiency and execution costs (Section II). It is therefore crucial to deploy appropriate selection strategies that attain the desired tradeoff. We mathematically formulate the problem of selecting the nodes so as to maximize the detection rate subject to not consuming more than a predetermined amount of resource (Section III-A). We prove that computing the optimal selection strategy is an NP-hard problem. Then, we present polynomial complexity approximation algorithms that attain constant factor approximation bounds (Section III-B). These algorithms however require recomputation every time the topology changes. Hence, we next propose heuristics that adapt seamlessly to topological changes (Section III-C). We evaluate the proposed algorithms using mathematical analysis and simulations (Section IV). In Section V, we describe the relevant literature. We prove the analytical results in the appendix.

The characterization of the optimal selection strategy allows us to identify the appropriate selection strategy for realizing desired tradeoffs between detection efficiency and resource consumption. Our investigation reveals that the approximation algorithms consume significantly lower resource as compared to heuristics when high detection rate is necessary, and thus must be deployed in this case. But, when the system can tolerate certain amount of intrusion and therefore the detection rate can be small, the heuristics and the approximately optimal strategies consume similar resource. Thus heuristics may be deployed in these scenarios. We develop analytical expressions that quantify the resource consumed by different selection strategies for any given detection rate. These expressions can therefore be used to decide which algorithm to deploy given the operating conditions. We also observe that the optimal algorithm detects all malicious packets by executing the IDS in a modest fraction of the nodes, even though it is oblivious towards the locations and identities of the intruders and the paths used by them. This is an encouraging outcome as in most ad hoc networks at least a small number of nodes will have significant energy. Thus, it would be sufficient to execute the IDS in only these nodes.

II. System Architecture

In this section, we describe our system assumptions.

We first postulate that ad hoc networks in near future will consist of two classes of nodes: (i) nodes that both communicate using the network and perform system tasks like relaying packets, discovering routes, securing communication, etc. (*insider nodes*), and (ii) nodes that only communicate using the network (*outsider nodes*). Our postulate is based on the observation that providing the desired quality of service to users is a pre-requisite for large scale use of this technology. But, if the network is to provide any quality of service (QoS) guarantee it can utilize the users but can not solely rely on them. This is because users may be available for short durations only. The QoS guarantees can however be provided if some easily deployable low complexity system nodes e.g., static and mobile access points are available. These nodes together with users who are trusted by the network and are in the network most of the time can be relied upon for performing system tasks. Such system nodes and trusted users therefore constitute the insiders. The remaining nodes are the outsiders.

We now provide several example wireless networks that consist of insiders and outsiders. During an event which is widely attended and lasts for short time, e.g., a super-bowl match, service providers may augment the connectivity and coverage provided by the existing cellular and/or Wi-Fi networks by utilizing additional static and mobile access points and the terminals of trusted users [13]. Here, the static and mobile access points as well as the trusted users constitute insider nodes. The remaining users who only communicate using the network are the outsiders. Mesh networks also consist of insiders (mesh points) and outsiders (users). In future, such networks may utilize some trusted users to perform system tasks, particularly during service outage due to failure of existing mesh points, or sudden and temporary increase in service demand in specific areas (temporary hot-spots) - such users would also constitute insiders. Finally, a disaster recovery team can use ad hoc networks to provide services like email, news, audio/video applications etc. in an area where communication infrastructure has been damaged due to a natural disaster or terrorist activity. The insider nodes are access points on buildings and mobile terminals carried by the personnel. The outsider nodes are civilians who communicate using the network.

All the above examples, and more generally the wireless networks with insiders and outsiders, retain the essential characteristics of ad hoc networks. These networks use multi-hop wireless communication, as source-destination paths may involve several insiders who relay messages using wireless links. Nodes in such networks, outsiders and also insiders, may be small mobile terminals and may have limited energy and memory, e.g., access points, laptops, personal digital assistants (PDAs) (insider nodes) carried by members of a disaster recovery team and trusted users. Static access points in some existing ad hoc networks in rural areas also have limited energy [4]. Finally, the set of insiders may change with time. For example, the network provider will need to provide incentive in lieu of service to the users who serve as insiders, and hence may utilize such users only as required, e.g., in hot-spots or when existing access points fail. We focus on detecting intrusion in these ad hoc networks. Note that these networks are significantly different from cellular networks where only the last hop is a wireless link, and only the nodes that use the network are mobile, dynamic and have limited energy and memory, while the set of nodes (base-stations) that perform system tasks remain the same, do not change locations and have practically unlimited energy and memory.

We now describe the security risks. An outsider may wish to deliver malicious (*bad*) packets to the destination, which may be an insider or an outsider, resulting in malfunction or failure of the destination. An outsider that sends bad packets is referred to as an intruder. A packet that is not *bad* is referred to as *good*. The network may have multiple intruders. The number and location of the intruders, their destinations and the paths used by them are not known to the network.

Intrusion can be detected if the destinations of the sessions (e.g., destinations $1, 2$ in figure 1) execute the IDS modules (host intrusion detection or HID) [15]. Here, a node executes the IDS at its application layer, and can therefore analyze only the packets it receives as destination, and not those that it relays. The advantage of HID is that it is not affected by the use of end-to-end cryptography or by changes in topology and routing that may be triggered by node mobility. But HID has several serious drawbacks. First, an intruder can avoid detection and produce maximum damage by exploiting the knowledge that only the destination analyzes the packets. For example if the intruder knows that the destination is using a particular version of Windows 2000 operating system, then it can transmit a packet that crashes the machine as soon as the destination's network layer assembles the packet and before the IDS at the application layer analyzes the packet [2]. Second, the detection mechanism will use the computation resources and network interfaces at the end-host. But, an attack on the target may simultaneously exhaust the resources available for detecting and reporting such attacks. Third, many of the destination nodes may not be able to execute the IDS due to limited computational resource and low residual energy. Finally, if only the end-hosts execute the IDS, then the bad packets would not be dropped until they reach the destination. Thus several nodes expend their limited energy and available bandwidth in relaying bad packets.

The network intrusion detection (NID) technique [15] executes the IDS on some selected insider nodes, e.g., the access point(2) in figure 1, which may be a relay or an end-host. Here, a node executes the IDS at its network layer, and can therefore analyze both the packets it relays and receives as destination. In ad hoc networks, NID has several advantages over HID. First, an intruder can no longer be certain that only the destination is executing the IDS. Moreover, the nodes that execute the IDS can be selected so that they have different characteristics. Thus, it will be more difficult for the intruders to devise attacks that are not detected. Second, these nodes can be selected only among those that have the required capability. Third, NID captures bad packets in transit and thus limits the wastage of bandwidth and energy in relaying them. Finally, the nodes that execute IDS can also analyze encrypted traffic when encryption is not at the network layer. For example, when traffic is encrypted at the application layer, IDS modules can detect attacks at transport and lower layers, e.g., ping-of-death, TCP SYN flood, smurf, bubonic, etc. If encryption is used at all layers, e.g., in battlefield networks, then schemes can be designed to distribute the keys securely to the nodes that execute the IDS. Investigation of key distribution schemes is beyond the scope of this paper. We consider NID in this paper.

Summarizing, *some selected insider nodes execute the IDS modules so as to detect bad packets while in transit between the intruder and its destination* - these are denoted as *IDS active*. Some insiders may not have the capability to execute the IDS. Thus, insiders are of two types: (a) *IDS capable* and (b) *IDS incapable*. Let V' be the set of IDS capable insiders. Only IDS capable insiders can become IDS active. The set of IDS active insiders changes with time since the selection depends on the topology. We assume that insider nodes are not compromised. Authentication mechanisms prevent an outsider from masquerading as an insider.

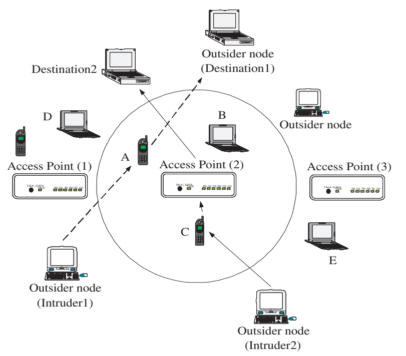


Fig. 1. This figure illustrates the system model. The outsider nodes (Intruder1, Intruder2) attack the destinations (1,2). The insider nodes are the access points, mobile terminals and laptops (B, D, E). If access point(2) is IDS active, it can hear the transmission from A, B and C and hence the attacks are detected.

We now examine the tradeoffs associated with different selection strategies. A straightforward strategy is to execute the IDS on every IDS capable insider. Thus every bad packet will be detected. But, the number of insiders is expected to be large. This is because of two reasons. First, since only insiders can relay packets, the insiders must constitute a non-negligible fraction of the total number of nodes in order to guarantee end-to-end connectivity and provide the desired throughput [25], and future networks will have a large number of nodes. Finally, executing IDS consumes significant resources like energy, memory and CPU cycles at each insider, and the insiders have limited resource. Thus, the straightforward strategy significantly increases the resource consumption in the system. On the other hand, if the IDS are executed in very few insiders, then the resource consumption decreases but some bad packets may escape inspection leading to undetected intrusion. *The challenge is to select the IDS active insiders so that the maximum possible number of packets are analyzed subject to consuming no more than a given amount of resource.*

We represent a wireless network by an undirected graph $G(V, E)$. Here, $V = \{1, \ldots, N\}$ consists of the insiders and E is the set of edges between the insiders. There exists an undirected edge between any two insiders that can receive transmissions from each other. We assume that every insider can receive its own transmission and hence has an edge to itself.

Definition 1: A *neighborhood* N_i of an insider node i is the set of insiders that have edges from i. An insider i *covers* every insider in its neighborhood. Let N'_i be the set of IDS capable neighbors of an insider i.

By this definition, an insider is always its own neighbor and covers itself.

An IDS active insider node operates in promiscuous mode, i.e., receives and analyzes any packet that is transmitted by any of its neighbors. For example, in figure 1, if access point(2) is

IDS active and operates in promiscuous mode, it can analyze the packets transmitted by nodes A, B, C. Clearly, operation in promiscuous mode increases the power consumption of these nodes. But, if no IDS active insider operates in promiscuous mode, then either a large number of insiders will need to execute the IDS, or several bad packets will not be captured. Our analysis and simulations demonstrate that the algorithms we propose attain high detection rate while executing the IDS in a modest fraction of the insiders; thus the operation of a small number of insiders in promiscuous mode consumes much less energy than executing the IDS in several insiders.

An attack may consist of a single packet (e.g., Code Red and Slammer [7]) or multiple packets (e.g., jolt2 or bubonic attacks). *We consider an attack to be detected when an IDS active insider analyzes all the packets that constitute the attack.* In our analysis, we assume that all packets constituting an attack traverse the same path. In this case, an IDS active insider analyzes all packets in an attack, if and only if it analyzes one packet in the attack. Therefore, without loss of generality, in the analysis we assume that each attack consists of a single packet. In our simulations we consider attacks with multiple packets and investigate the impact of path changes. Note that when insiders aggregate each others analysis then an intrusion can be detected even when different IDS active insiders examine different packets of the same attack. But such aggregation requires significant message exchanges and increases the complexity and the resource consumed in the detection [20], [29]. The design of efficient schemes for complete or partial aggregation is a topic of future research. We therefore do not assume the existence of such schemes.

III. Intrusion detection in presence of resource limitation

We consider the problem of selecting the IDS active insiders so as to maximize the detection efficiency subject to maintaining resource consumption below the desired value. In subsection III-A, we motivate and subsequently mathematically formulate the detection objective. We prove that this problem is NP-hard. In subsection III-B, we present a polynomial complexity algorithm for approximating the optimal solution within a provable approximation bound. This algorithm is oblivious to the movement of outsider nodes, but requires recomputation whenever insider nodes move. In subsection III-C, we present algorithms that do not have provable approximation bounds, but nevertheless do not require such recomputations and are therefore more suitable when insider nodes move rapidly. All the algorithms proposed in this section are oblivious towards locations, identities of the intruders and the paths used by them.

A. Selecting the IDS active insiders for maximizing the detection efficiency subject to bounded resource consumption

We consider the goal of selecting the IDS active insiders among the IDS capable insiders such that the detection efficiency is maximized subject to limiting the resource consumed for detecting intrusion. We first quantify the resource consumed by any selection strategy. We subsequently quantify the detection efficiency of any selection strategy. We next formulate the detection goal as an optimization problem and prove that optimally selecting the IDS active insiders is NP-hard.

We first describe the resource consumed by each IDS active insider. An IDS active insider needs to receive and analyze all packets transmitted in its neighborhood. Thus, it needs to constantly operate in active mode which consumes significant energy. Next, traffic analysis is computationally intensive, e.g., a P3 850 MHz laptop spent 10% CPU cycles to analyze 1.5 Mbits per second [25]. The CPU usage of an IDS active insider increases further with the increase in traffic transmitted in the insider's neighborhood. Finally, an IDS active insider must store the traffic analysis module and the signature database; these occupy significant part of its memory, e.g., in a Windows-based system a commonly used collection of signatures, Snort, consumes 256MB of memory [3]. Furthermore, each IDS active insider consumes resource from the system, and introduces additional system complexity. First, each IDS active insider u needs to regularly update the signatures by downloading them from a central database which consumes bandwidth, energy and memory at all insiders in the path between u and the database, and the update frequency can be as much as once every 30 minutes [1]. Next, whenever an IDS active insider generates a report to the security administrator or a neighboring node, regarding an attack or lack thereof, it must authenticate itself. Thus, these insiders must maintain and periodically update the authentication keys; such updates consume communication resources from other nodes. Finally, the IDS active insiders may demand some incentives from the system, for agreeing to perform the required tasks. Clearly, the total system resource consumed in the detection process, which includes resource consumed at the IDS active and the IDS inactive insiders and the incentive demanded by the IDS active insiders increases with increase in the number of the IDS active insiders. We therefore consider the resource consumed by the selection strategy as the number of IDS active insiders. Motivated by the need to reserve a part of the network resources for other functions, we impose the constraint that a detection strategy should have at most n IDS active insiders, where n is a system parameter.

We now quantify the detection efficiency of a selection strategy. Since an IDS active insider detects bad packets transmitted by its neighbors, all bad packets will be detected if all intruders are covered by the IDS active insiders. This is difficult to attain because the network has a large number of outsiders and only a small fraction of these are intruders, and the network does not know apriori the identity and the location of any outsider; the number and location of the outsiders also change rapidly. Now note that all bad packets are relayed by insiders except those that are directly transmitted from the intruders to their target nodes. This is because only insiders relay packets. Thus, the detection efficiency increases when the IDS active insiders cover larger number of insiders. We consider the detection efficiency of a strategy to be the number of insider nodes covered by IDS active insiders.

Thus, *our goal is to select the IDS active insider nodes among the IDS capable insider nodes such that they cover* *the maximum possible number of insider nodes subject to constraining the total number of the IDS active insider nodes to be upper bounded by a constant n.* We refer to a selection algorithm that attains the above objective as the optimal algorithm.

Lemma 1: Optimally selecting the IDS active insiders is an NP-hard problem.

Proof: We first describe the maximum coverage problem which is a well-known NP-hard problem (Section 3.9 [10]). There exists a set U with elements $\{u_1, \ldots, u_N\}$ and K subsets of U: $U_1, \ldots, U_K$. The maximum-coverage problem is to select n of these subsets so that the union of the selected subsets has the maximum possible cardinality. Consider a wireless network with IDS capable insiders $v_1, v_2, \ldots, v_K$ and IDS incapable insiders $u_1, \ldots, u_N$. Thus, $V = \{v_1, \ldots, v_K, u_1, \ldots, u_N\}$. Let $E = \{(v_i, u_j)$ if $u_j \in U_i\} \cup \{(a,a), a \in V\}$. Thus, $N_{v_i} = v_i \cup U_i$. Let the upper bound on the number of IDS active insiders be n in this network. The optimal selection strategy selects n IDS capable insiders $v_{i_1}, \ldots, v_{i_n}$ such that $|N_{v_{i_1}} \cup \ldots \cup N_{v_{i_n}}| = \max_{T \subseteq \{1,\ldots,K\}, |T|=n} | \cup_{j \in T} N_j|$. Note that for any $T \subseteq \{1, \ldots, K\}, |T| = n$, $| \cup_{j \in T} N_{v_j}| = | \cup_{j \in T} U_j| + n$. Thus, $U_{i_1} \ldots \cup U_{i_n}$ constitute the optimal solution for the maximum coverage problem as well. Thus, if the optimal set of IDS active insiders can be determined in polynomial complexity, then the maximum coverage problem can also be solved in polynomial complexity. ∎

Lemma 1 also holds in the special case that all insiders are IDS capable [25].

The optimal set of IDS active insiders can be computed by solving an integer linear program, MDBR_{IP} (maximize detection subject to bounded resource consumption). For each insider node $i \in V$ there exists two integer variables: (a) x_i and (b) y_i. Now, x_i indicates whether an IDS active node covers i, i.e., $x_i = 1$ if an insider node in N_i' is IDS active, and 0 otherwise. Also, $y_i = 1$ if i is IDS active, and 0 otherwise. Thus, $x_i = \min(1, \sum_{j \in N_i'} y_j)$. Thus, since each y_j is a non-negative integer, x_i is either 0 or 1. The upper bound on resource consumption introduces another constraint: $\sum_{j \in V} y_j \leq n$. The goal of MDBR_{IP} is to maximize the number of insiders covered by the IDS active insiders, i.e., $\sum_{j \in V} x_j$ subject to these constraints.

(MDBR_{IP}) Maximize: $\sum_{j \in V} x_j$

subject to

1) $x_i \leq \sum_{j \in N_i'} y_j, \ \forall\, i \in V$,
2) $x_i \leq 1, \ \forall\, i \in V$,
3) $y_i \in \{0, 1\}, \ \forall\, i \in V$,
4) $\sum_{j \in V} y_j \leq n$.

An integer linear program (ILP) can be solved in exponential complexity, which is expected since the optimal selection is an NP-hard problem.

We end this subsection with a few concluding remarks. First, in Section IV, we quantify the probability of detection of an attack under the optimal selection strategy. Next, the detection goal can be generalized to accommodate a more general quantification of the resource consumed by any selection strategy. We can assign an IDS capable insider i weight w_i, and consider the resource consumed by a selection strategy to be the sum of the weights of all IDS active insiders. The goal now is to maximize the detection efficiency subject to ensuring that the resource consumed does not exceed n. This generalization would allow us to associate different importance with the resource consumed by different insiders e.g., laptops, PDAs, by assigning different weights to different nodes, based on their residual energy and computational capability. The above ILP can easily be generalized to optimally select the IDS active insiders in this case; the optimal selection problem continues to remain NP-hard. Our simplification has been to assume that $w_i = 1$ for all i.

B. Algorithms for approximating the optimal solution within guaranteeable approximation bound

We now present two polynomial complexity algorithms that approximately compute the optimal set of IDS active insiders. The first algorithm, Greedy-MC (Greedy algorithm for maximum coverage), has been adapted from a known approximation algorithm for the maximum coverage problem in arbitrary graphs [10]. Greedy-MC attains the best possible approximation ratio that can be attained by any polynomial complexity algorithm, but requires several network-wide communications; the number of these communications increase with increase in values of system parameters. We next design a polynomial complexity approximation algorithm "Maximum Unsatisfied Neighbors in Extended Neighborhood for Maximum Coverage" (MUNEN-MC) that selects the same set of nodes as Greedy-MC, but requires only a constant number of network-wide communications [24].

We now describe Greedy-MC. We first introduce a new notion.

Definition 2: The *priority* of an insider node is the number of its neighbors that are not covered by any IDS active insider.

Greedy-MC iteratively selects the IDS active insiders. In each iteration, it selects an IDS capable insider v that has (a) positive priority and (b) the maximum priority among all IDS capable insiders[§]. After the selection, every insider in v's 2-hop neighborhood recomputes its priority. The selection process terminates either when all the IDS capable insiders have priority 0 or at the end of n iterations, whichever occurs earlier. Thus, Greedy-MC has $O(nN)$ complexity.

Figure 2 elucidates the operation of Greedy-MC (and MUNEN-MC).

Greedy-MC selects s IDS active insiders among the IDS capable insiders such that (a) $s \leq n$ and (b) the IDS active insiders cover at least $1-(1-1/n)^n$ times that of the maximum number of insiders covered by any n IDS capable insiders. This guarantee holds because Greedy-MC always selects an insider in iteration j $(1 \leq j \leq n)$ such that the cardinality of the union of the neighborhoods of all selected insiders is the maximum possible given that the selection of the insiders in previous iterations cannot be changed. Now, it is well-known that the number of elements in the union of n subsets selected as above, from any given collection of subsets, is at least $1 - (1 - 1/n)^n$ times that of the maximum number of elements in the union of any n subsets in the collection [10].

[§]If multiple IDS capable insiders have the maximum priority, Greedy-MC selects the one with the least identity among them.

As Lemma 1 demonstrates, the optimal selection problem is an instance of the maximum coverage problem. Unless $P = NP$, the best possible approximation ratio for the maximum coverage problem is $1 - 1/e$. Specifically, unless $P = NP$, given an $\epsilon > 0$, it is possible to construct a collection of subsets such that no polynomial complexity algorithm can be guaranteed to select n among them such that the cardinality of the union of the selected subsets exceeds $1 - 1/e + \epsilon$ times that of the optimal selection [10]. Thus, $1 - 1/e$ is the best possible approximation ratio for the selection problem. Now, $1 - (1 - 1/n)^n \geq 1 - 1/e$. Thus, Greedy-MC attains the best possible approximation ratio.

The problem with Greedy-MC is that before the selection of each IDS active insider it needs network-wide communications to determine which insider has the highest priority in the network. Thus, it requires $O(n)$ network-wide communications.

We design another polynomial complexity approximation algorithm, MUNEN-MC that selects the same set of nodes as Greedy-MC, but has significantly lower communication complexity than Greedy-MC - MUNEN-MC requires only 3 broadcasts, irrespective of n.

We now describe MUNEN-MC. MUNEN-MC sequentially executes the following two phases: (i) node-selection and (ii) node-retention. During the node-selection phase, in each iteration an IDS-capable insider u selects itself if

- u has positive priority¶ and
- for any IDS capable insider v in u's 2-hop neighborhood, either (i) u's priority is greater than that of v or (ii) u and v have equal priority and $u < v$.

At the end of each iteration (i.e., after the selections in the iteration), nodes recompute their priorities. The node-selection phase continues for n iterations, and is followed by the node-retention phase.

We now describe the node-retention phase. We first define the notion of "select-priority", which is the priority of a node selected during the node-selection phase just before it is selected. During the node-retention phase, n nodes with highest select-priorities are retained; the rest of them are eliminated. If two selected nodes have equal select-priorities, then the node with lower identity is preferred. The nodes retained at the end of this phase are selected as IDS active insiders.

Clearly, MUNEN-MC uses only local communication during the node-selection phase. We now describe how a constant (3) number of broadcasts can be used to discover which n insiders have the largest priorities. Some pre-determined root insider broadcasts a query packet along a spanning tree. The query packet has n tuples, and initially each tuple has value $(0, 0)$. Let v be the insider with the least priority in the list. If insider u's priority is higher than that of v, or equal to that of v and $u < v$, u includes its identity and select-priority, and removes the entry corresponding to v. Finally, insiders at the leaves of the spanning tree return the query packet towards the root which re-broadcasts the query packet. Thus, every insider knows which insiders would be retained.

¶Once an insider selects itself, in all subsequent iterations it has 0 priority and hence does not select itself again.

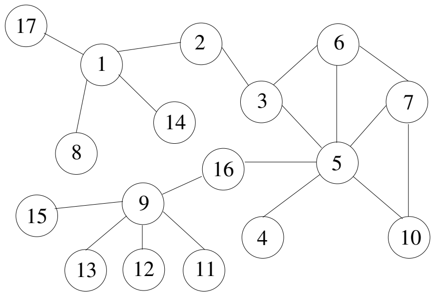


Fig. 2. Let $n = 2$ and let all insiders be IDS capable. Greedy-MC selects insiders 5 and 1 in the first two iterations respectively. Now, consider MUNEN-MC. The node-selection phase continues for 2 iterations. In the first iteration, insiders 5 and 1 are selected. In the second iteration, insider 9 is selected. The select-priorities of insiders $5, 1, 9$ are $7, 5, 5$ respectively. During the node-retention phase, nodes 5 and 1 are retained.

Theorem 1: MUNEN-MC selects the same set of IDS active insiders as Greedy-MC.

Thus, MUNEN-MC attains the best possible approximation ratio as well.

The analysis and simulations demonstrate that when all insiders are IDS capable, both the optimal and approximation algorithms attain very high probability of detection (close to 1). This is remarkable since both these algorithms are oblivious to the location and identity of the intruders and the paths used by them.

C. Robust heuristic algorithms for selecting the IDS active insiders when insider nodes move

The algorithms presented so far are oblivious to the position of outsiders, and are therefore not affected by their movements. But, the IDS active set must be recomputed each time an insider's neighborhood changes due to its or its neighbors' movements. Every such recomputation involves at least 3 network-wide broadcasts. Thus, these algorithms cannot be used when insider nodes move rapidly as then the recomputations are frequent. We now present computationally simple heuristic selection strategies that do not require any re-computation with movement of either insider or outsider nodes, and require only limited message exchange when insiders move. The disadvantage is that the heuristics consume more resource for attaining the same probability of detection as compared to the optimal and approximation algorithms.

First, we consider a naive algorithm, *Random Placement (RP)*, in which every IDS capable insider executes the IDS with a probability which can be selected so as to regulate the resource consumed and detection probability. For example, if this probability is high, then a large number of insiders are IDS active. Thus, the detection consumes a lot of resource but most bad packets are detected.

We now propose another heuristic, which we refer to as GO-DOM (geometric dominating set algorithm), that uses geometric information to select the IDS active insiders (Figure 3). This heuristic can be used in topologies where all insiders have equal transmission ranges, which we denote as r. Thus, two insiders are neighbors if and only if the distance between them is less than or equal to r. The network is covered by the minimum possible number of circles each with radius r. Each

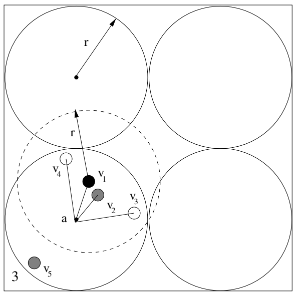


Fig. 3. This figure illustrates the operation of GO-DOM. The circles in solid lines are some of those that cover the geographic area of the network. For the current positions of the nodes, 2 nodes in circle 3, v_2, v_5, execute the IDS. Both v_2 and v_5 are the nearest in their neighborhoods to the center a of the circle they reside in, i.e., circle 3. Now, v_1 does not execute IDS as v_2 in v_1's neighborhood (the dashed circle) is nearer to a than v_1.

IDS capable insider knows or computes the coordinates of the centers of the circles. Note that this is a one time computation or message exchange for each IDS capable insider. We assume that each insider knows its coordinates (e.g., by using GPS or other existing techniques [5]). An insider selects an IDS capable neighbor which is the nearest to the center of a circle it currently resides in to execute the IDS (an insider may select itself as well since by definition it is its own neighbor). For this, each IDS capable insider broadcasts its distance from the center of each circle it resides in to its neighbors. It sends this broadcast packet when it joins the system, and thereafter each time it moves.

GO-DOM detects all bad packets as it selects the IDS active insiders so as to cover the entire network. We now generalize GO-DOM so as to select fewer IDS active insiders at the expense of obtaining lower detection rates. Now, each insider selected by GO-DOM decides whether to execute the IDS with a probability which can be selected so as to regulate the resource consumed and detection rate. We refer to this version as generalized geometric dominating set algorithm (GGO-DOM).

In the next section, we compare the performances of the heuristics with the optimal and approximation algorithms, and determine when each may be deployed.

IV. Performance Evaluation

Using analysis and ns2-simulations, we compare the performance of the optimal and approximation algorithms and the computationally simple heuristics. This comparison allows us to evaluate the benefits of (approximately) optimally selecting the IDS active insiders, and accordingly decide the appropriate algorithm for any desired tradeoff between detection probability and resource consumption. We first obtain computationally simple analytical expressions for the performance of the optimal algorithm (subsection III-A) and RP in a network with static insiders. Then we simulate the performance of the approximation algorithm and RP and compare the results obtained from analysis and simulation. These comparisons validate both the analysis and the simulations and also demonstrate that the approximation and the optimal algorithms perform similarly. Finally, in networks with mobile insiders we compare the performance of GGO-DOM and RP using simulations.

For each algorithm, we first analyze the probability of detection of bad packets at each insider. The analysis is exact for RP, but provides bounds for the optimal algorithm. We then consider the probability of detection of an attack when the bad packets traverse arbitrary number of hops between the intruder and its target. This generalization is complicated and we obtain only approximate results for both algorithms.

We now describe the first analysis. We assume that N static insiders are uniformly distributed in a square of area A. Each insider is IDS capable. Now we assume that an insider u can receive transmissions from any node v which is within a distance r from u. Thus, the fraction of total area covered by an insider is $\rho = \pi r^2/A$. We refer to this model as the "ETICUS(N, ρ)" ("all insiders have equal transmission ranges, are IDS capable and uniformly distributed in a square") model. The optimal algorithm executes IDS in n insiders so as to maximize the number of insiders covered by IDS active insiders. RP executes IDS in each insider with probability (w.p.) q. As discussed before, without loss of generality, we assume that each attack consists of a single bad packet. A bad packet is analyzed and hence detected by an IDS active insider if it is relayed by at least one neighbor of the insider. Depending on the value of n and q, all insiders need not be covered by IDS active insiders, and thus all bad packets will not be detected. We compute the probabilities of detection of the bad packets while being relayed by a uniformly selected insider for the optimal algorithm ($P_D^{\text{OPT}}(N, n, \rho)$) and RP ($P_D^{\text{RP}}(N, q, \rho)$) as functions of n and q respectively for any given values of parameters N, ρ.

First, consider the simple case that $\rho << 1$. In this case, we can ignore the "edge effects," i.e., we assume that each insider's coverage area is within the overall area. Now, the probability that a bad packet is not detected while being relayed by an insider u is the probability that none of u's neighbors is IDS active; this probability is $(1-q)(1-q\rho)^{N-1}$. Thus,

$$P_D^{\text{RP}}(N, q, \rho) \approx 1 - (1-q)(1-q\rho)^{N-1} \text{ if } \rho << 1. \quad (1)$$

Now, (1) provides important insight about RP's selection strategy for different q. Note that $P_D^{\text{RP}}(N, q, \rho)$ increases linearly with increase in the total area covered by the IDS active insiders. When $q << 1$, this area is small. Now, since the IDS active insiders are uniformly distributed under RP, and since the uncovered area is more than the covered area, a new IDS active insider is more likely to be selected in the uncovered area. Thus, for low q, RP selects the IDS active insiders such that their coverage areas minimally overlap. Thus, the coverage area should increase approximately by ρA whenever a new IDS active insider is added. Hence, $P_D^{\text{RP}}(N, q, \rho)$ should increase linearly with increase in each of the variables N, q, ρ when the other two variables do not change. Consistent with this intuition, it follows from (1) that

$$P_D^{\text{RP}}(N, q, \rho) \approx (N-1)q\rho \text{ if } \rho << 1, q << 1. \quad (2)$$

Now, when q is high, the IDS active insiders together cover a large area. Now, since the IDS active insiders are uniformly distributed under RP and since the covered area is more than the uncovered area, a new IDS active insider is more likely to be selected in the covered area. Thus, RP selects the IDS active insiders such that their coverage areas significantly overlap, and hence the above linear approximation does not apply.

The following theorem relaxes the assumption that $\rho << 1$ and provides $P_D^{\text{RP}}(N, q, \rho)$ for arbitrary q, ρ, N.

Theorem 2:

$$
\begin{aligned}
&g(x, y) \\
&= 1 - \frac{\cos^{-1}(x) - x\sqrt{1-x^2} + \cos^{-1}(y)}{\pi} \\
&\quad - \frac{y\sqrt{1-y^2} + 0.5(\sqrt{1-y^2} - x)(\sqrt{1-x^2} - y)}{\pi} \\
&\quad + \frac{|\pi/4 - \left(\cos^{-1}(x) + \cos^{-1}(y)\right)/2|}{\pi} \\
&\quad - \frac{0.5\sqrt{1 - x^2 - y^2 + 2x^2y^2 - 2xy\sqrt{(1-x^2)(1-y^2)}}}{\pi}.
\end{aligned}
$$

$$
\begin{aligned}
&P_D^{\text{RP}}(N, q, \rho) \qquad (3) \\
&= 1 - (1-q)[(1-q\rho)^{N-1}\left(1 + \frac{4\rho}{\pi} - 4\sqrt{\frac{\rho}{\pi}}\right) \\
&\quad + \left(4\sqrt{\frac{\rho}{\pi}} - 8\frac{\rho}{\pi}\right) \times \\
&\quad \int_0^1 \left(1 - q\rho\left(1 - \frac{\cos^{-1}(x)}{\pi} + \frac{x}{\pi}\sqrt{1-x^2}\right)\right)^{N-1} dx \\
&\quad + \frac{4\rho}{\pi}\int_0^1\int_0^1 (1 - q\rho g(x,y))^{N-1}\, dx dy]. \qquad (4)
\end{aligned}
$$

When $\rho << 1$ the integrations are close to 1 and thus, (4) reduces to (1).

Note that it is difficult to compute $P_D^{\text{OPT}}(N, n, \rho)$ because of the dependence between the selection of the IDS active insiders and the topology. So, we obtain a stochastic upper bound for $P_D^{\text{OPT}}(N, n, \rho)$. Given N, ρ, we compute this upper bound by computing a lower bound for the minimum n required to attain a desired $P_D^{\text{OPT}}(N, n, \rho)$. We also obtain an approximation which we intuitively argue as a lower bound for $P_D^{\text{OPT}}(N, n, \rho)$. Using numerical computations, we would show that the bounds are close to each other suggesting that both are good approximations for $P_D^{\text{OPT}}(N, n, \rho)$.

Theorem 3: Let $B(L, g, j)$ be the tail probability of a binomial distribution with parameters L, g, i.e.,

$$B(L, g, j) = \sum_{i=j}^{L} \binom{L}{i} g^i (1-g)^{L-i}.$$

Let P be the required probability of detection and let $(x)_- = \min(x, 1)$. For any given ϵ, $0 < \epsilon < 1$, with a probability of at least $1 - \epsilon$ the number of IDS active insiders, n, required by the optimal algorithm to attain $P_D^{\text{OPT}}(N, n, \rho) = P$ exceeds $n_{\text{LB}}^{\text{OPT}}(N, \rho)$, where

$$
\begin{aligned}
&n_{\text{LB}}^{\text{OPT}}(N, \rho) \\
&\quad = \max_{l: l \le \lceil NP \rceil} \left\{ l : \binom{N}{l} B\left(N, (l\rho)_-, \lceil NP \rceil - l\right) < \epsilon \right\}.
\end{aligned}
$$

We now consider another approximation for $P_D^{\text{OPT}}(N, n, \rho)$ which is computed assuming that every point in the square under consideration is an insider. This resembles a network with a large number of insiders. We refer to this assumption as the ETICDS(ρ) model (all insiders have equal transmission ranges, are IDS-capable and densely distributed in a square). We investigate the maximum possible probability of detection $P_D^{\text{OPT}}(n, \rho)$ when n insiders execute IDS in such a network. Note that $P_D^{\text{OPT}}(n, \rho)$ does not depend on N. Intuitively, in the ETICUS(N, ρ) model fewer insiders need to be covered using n IDS active insiders than in the ETICDS(ρ) model and thus bad packets are detected with a higher probability in the former. Thus, we expect $P_D^{\text{OPT}}(N, n, \rho) \ge P_D^{\text{OPT}}(n, \rho)$. Computing $P_D^{\text{OPT}}(n, \rho)$ is again difficult as it requires the characterization of the maximum possible area covered by n discs of radius r in a square of area A, which to the best of our knowledge, is an open problem in mathematics. Asymptotic upper bounds for this maximum possible area is however known [27]. We could however lower bound $P_D^{\text{OPT}}(n, \rho)$ for any n, ρ. This provides a lower bound for $P_D^{\text{OPT}}(N, n, \rho)$.

Theorem 4: Let $\sqrt{\pi/\rho}$ be an even integer.

$$
P_D^{\text{OPT}}(n, \rho)
\begin{cases}
= n\rho, \text{ if } n \le \frac{\pi}{4\rho} \\
\ge \frac{\pi}{4} + (n - \frac{\pi}{4\rho})\frac{\rho(4-\pi)}{\pi}, \\
\text{if } \frac{\pi}{4\rho} < n \le \frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1 \\
\ge 1 + \left(n - (\sqrt{\frac{\pi}{\rho}} + \frac{\pi}{2\rho} - 1)\right)\frac{\rho(4-\pi)}{2\pi}, \\
\text{if } \frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1 < n \le \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3 \\
\ge 1 + \left(n - (\sqrt{\frac{\pi}{\rho}} + 1 + \frac{\pi}{2\rho})\right)\frac{\rho(4-\pi)}{4\pi}, \\
\text{if } n > \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3.
\end{cases}
$$

Theorem 4 shows that given ρ, the lower bound on $P_D^{\text{OPT}}(n, \rho)$ is a piece-wise linear function of n. This happens because the optimal algorithm selects the IDS active insiders such that their coverage areas minimally overlap - this maximizes the detection probability. Thus, each additional IDS active insider increases the coverage area and hence the detection probability by similar amount. Refer to technical report [25] for the lower bound for $P_D^{\text{OPT}}(n, \rho)$ when $\sqrt{\pi/\rho}$ is not an even integer.

We now compare the above analytical expressions with measurements obtained using ns2-simulations. In our simulations, we consider topologies with insiders distributed as per the ETICUS(N, ρ) model with $N = 400$, $\rho = 0.087, 0.1963$ ($r = 100, 150$ m), $A = 600^2 m^2$. In each case, we consider 200 different trials. In each trial, an attack consisting of 10 packets is launched and a uniformly selected insider relays the packet. The probability of detection is measured as the percentage of trials in which the attack is detected while the bad packets are relayed by the selected insider; an attack is detected if all packets constituting the attack are received by an IDS active insider. Note that computing the optimal set of IDS active insiders for $N = 400$ requires substantial time, which is expected given that the optimal selection problem is NP-hard. Thus, for the simulations, we execute IDS in the insiders selected by the approximately optimal algorithm, MUNEN-MC. We justify this approximation as follows. We computed an upper bound for the number of insiders covered by the optimal set of IDS active insiders by relaxing the integer constraints in MDBR_{IP}. For different topologies this upper bound exceeds the number of insiders covered by the

IDS active insiders selected by MUNEN-MC only by a small amount. For example, for $\rho = 0.087$, for different values of n, the two numbers differ by at most 4% of the former [25]. In RP the expected number of IDS active insiders is Nq. Thus, for even comparison with the optimal algorithm, we select $q = n/N$.

In Figures 4 (a) and (b) we plot the probabilities of detection measured from simulation and that obtained from the analytical expressions ($P_D^{\text{RP}}(N, n/N, \rho)$ obtained from Theorem 2 and the upper and lower bounds for $P_D^{\text{OPT}}(N, n, \rho)$ obtained from Theorems 3 and 4 respectively) as a function of the expected number[‖] of IDS active insiders, n, for different values of ρ. For the upper bound, we select $\epsilon = 0.1$, i.e., the upper bound holds w.p. 0.9. These plots demonstrate that the results obtained from the simulation and the analysis match closely. For the optimal algorithm, the upper and lower bounds are close indicating that both are good approximations, and as expected the detection probability measured in the simulation is between the two bounds. In Figure 4 (c) we plot the ratio between the expected number of IDS active insiders of RP and the optimal solution as a function of the probability of detection. We obtain this ratio from simulation measurements. Figure 4 (c) shows that for high detection probabilities, the number of insiders required by RP is significantly higher than that by the optimal algorithm. But for low detection probabilities, both algorithms require similar number of IDS active insiders. Thus, given its low resource consumption, the optimal algorithm (or its approximation MUNEN-MC) is a clear choice when systems require very high detection probabilities (e.g., $> 95\%$). Given its simplicity, RP is a clear choice for systems that can accept low detection probabilities.The thresholds for these "low, medium, high" detection probabilities can be computed from the analytical expressions.

We now explain these observations using the analysis. For low detection probability, n and q are both low. Thus, from (2) and Theorem 4, since $N >> 1$ and $q = n/N$, $P_D^{\text{RP}}(N, n/N, \rho) \approx n\rho = P_D^{\text{OPT}}(n, \rho)$. When the number of insiders (N) is large, $P_D^{\text{OPT}}(n, \rho)$ is a good approximation for $P_D^{\text{OPT}}(N, n, \rho)$. Thus, at low detection probability, RP and the optimal have similar performance. For high detection probability, q is high. Hence, as discussed before, unlike the optimal algorithm, RP selects the IDS active insiders such that their coverage areas significantly overlap. Therefore, compared to the optimal algorithm, RP has much smaller increase in coverage area and hence detection probabilities for the same increase in the number of IDS active insiders. Conversely, at high detection probability, for equal increase in detection probability, compared to the optimal algorithm, RP needs to execute the IDS in many more insiders.

We now allow bad packets to traverse arbitrary number of hops between the intruder and its target and obtain approximate results for the probabilities of detection of the attacks for both the optimal algorithm and RP. We point out the approximations after each result. We now assume that the insiders are uniformly distributed in a circle of radius R and area A. Thus $A = \pi R^2$, and $\rho = \pi r^2 / A$. The intruder and its target are uniformly distributed in the circle. Thus multiple insiders may relay the packets. The rest of the assumptions remain the same. As before, we approximately compute the probabilities of detection of an attack for the optimal algorithm ($P_D^{\text{OPTM}}(N, n, \rho)$) and RP ($P_D^{\text{RPM}}(N, q, \rho)$) as functions of n and q respectively for any given values of parameters N, A, ρ (the letter M indicates possible multihop transmissions).

Theorem 5:

$$\begin{aligned}
& P_D^{\text{RPM}}(N, q, \rho) \\
\approx\ & 1 - 16/\pi\Big[\int_0^{\frac{\sqrt{\rho}}{2}} (1 - q\rho)^N (z\cos^{-1}(z) - z^2\sqrt{1 - z^2})dz \\
& + \int_{\frac{\sqrt{\rho}}{2}}^{1} (1 - q)^{\lceil \frac{2z}{\sqrt{\rho}} - 1 \rceil} \times \\
& \left(1 - q\rho\left(\lceil \frac{2z}{\sqrt{\rho}} \rceil (1 - \frac{1.228}{\pi}) + \frac{1.228}{\pi}\right)\right)^{N - \lceil \frac{2z}{\sqrt{\rho}} - 1 \rceil} \\
& \times (z\cos^{-1}(z) - z^2\sqrt{1 - z^2})dz\Big].
\end{aligned}$$

The approximation here is that we ignore the "edge effects". The edge effects arise only for insiders that are at a distance greater than $R - r$ from the center of the circle. But, the resulting inaccuracy is negligible when $\rho << 1$, which is normally the case.

We now approximate $P_D^{\text{OPTM}}(n, \rho)$, which is the probability that an attack is detected when every point in the simulation area is an insider. As before, we expect $P_D^{\text{OPTM}}(N, n, \rho) \geq P_D^{\text{OPTM}}(n, \rho)$.

Theorem 6:

$$\begin{aligned}
& P_D^{\text{OPTM}}(n, \rho) \\
\geq\ & \begin{cases}
\left(1 - \frac{4\rho n}{\pi}\right) \int_{2\sqrt{\frac{n}{\pi}}}^{\sqrt{\frac{1}{\rho}}} \Big[\Big(1 - \frac{1}{\pi}\cos^{-1}\left(2\sqrt{\frac{n\rho}{\pi}}\right) \\
-\frac{1}{\pi}\cos^{-1}\left(\frac{2}{z}\sqrt{\frac{n}{\pi}}\right)\Big) \\
+\frac{2}{\pi}\sqrt{\frac{n\rho}{\pi}\left[1 - \frac{4n\rho}{\pi}\right]} + \frac{4\rho n}{\pi^2}\cos^{-1}\left(\frac{2}{z}\sqrt{\frac{n}{\pi}}\right)\Big] 2\rho z dz \\
+\frac{4\rho n}{\pi}\Big[1 - \frac{(4-\pi)\rho}{4\pi n}\{(4 - \pi)(n + 1 - \sqrt{n\pi}) \\
+ \left[\sqrt{n\pi} - \frac{\pi}{2}\right]\Big[\frac{4-\pi}{2} + \frac{1}{\rho}\cos^{-1}\left(2\sqrt{\frac{n\rho}{\pi}}\right) \\
-\frac{2}{\pi}\sqrt{\frac{n(\pi - 4n\rho)}{\rho}}\Big]\}\Big], \text{ if } n \leq \frac{\pi}{4\rho} \\
1 + \left(n - (\frac{\pi}{2\rho} - \frac{\pi}{4} - \frac{\pi}{4\sqrt{\rho}} + 1)\right)\left(\frac{\rho(4-\pi)}{\pi}\right)^2, \\
\text{if } \frac{\pi}{4\rho} < n \leq \frac{\pi}{2\rho} - \frac{\pi}{2\sqrt{\rho}} + 1 \\
1 + \left(n - (\frac{\pi}{2\sqrt{\rho}} + \frac{\pi}{2\rho} - \pi + 1)\right)\left(\frac{\rho(4-\pi)}{2\pi}\right)^2, \\
\text{if } n > \frac{\pi}{2\rho} - \frac{\pi}{2\sqrt{\rho}} + 1.
\end{cases}
\end{aligned}$$

We now compare the above analytical expressions with measurements obtained using ns2-simulations. Again, the insiders are distributed as described in the analysis, and $R = 300$ m. The rest of the parameters are selected as in the previous simulation. The route between the intruder and its destination is selected using two different routing algorithms - AODV and DSR. Figures 4 (d) and 4(e) demonstrate that the results obtained using analysis and simulation match well - the differences are somewhat more than in the previous case. This is because of the additional approximations in this case. But, again the discrepancies are not significant. Also, as

[‖]For RP, each insider executes the IDS w.p. q and hence n represents the expected number of IDS active insiders selected by RP. For the optimal algorithm, n is the exact number of IDS active insiders.

expected both algorithms have higher detection probabilities than in the previous case. This is because the bad packets travel longer paths and are thus more likely to travel through the neighborhood of IDS active insiders. Figure 4(f) shows that the performance difference between RP and the optimal algorithm is as before. Also, the choice of the routing algorithm does not affect the detection rate. Finally, an intruder may send bad packets directly to its target node without using an intermediate insider as a relay. But, still the optimal algorithm can attain very high probability of detection for moderate n. This happens because even when n is moderate the intruder is likely to be in the transmission range of some IDS active insider which detects the bad packets the intruder transmits.

In Figure 5 we plot the probability of detection as a function of ρ at different values of n for both algorithms. We consider both (a) the probability of detection at each insider and (b) probability of detection of an attack. We obtain the plots using the analytical expressions given in Theorems 2, 4 (case (a)) and Theorems 5 and 6 (case (b)). As expected, for both algorithms the probability of detection at any given n increases with increase in ρ. This is because with increase in ρ each IDS active insider covers a larger area and hence larger number of insiders and hence is more likely to detect bad packets. The plots suggest that for both algorithms the probability of detection can be approximated by piece-wise linear functions of ρ.

Now, we compare the performance of GGO-DOM and RP (subsection III-C) when all nodes are mobile. Recall that the optimal and approximation algorithms (subsections III-A and III-B) cannot be used in this case as the solutions must be recomputed every time an insider moves. We select the probabilities in GGO-DOM and RP so as to have the desired value of the expected number of IDS active insiders. We consider topologies where 100 IDS capable insiders, 5 intruders and 5 destinations are uniformly distributed in a square of side 670 m. Each intruder launches an attack consisting of 10 packets on a separate destination. Each attack is detected if and only if all packets constituting the attack are received by an IDS active insider. The probability of detection of an attack is measured as the fraction of attacks that have been detected over all trials. Each node moves as per the random way point mobility model with maximum speed of 20 m/s and pause time 10 sec. The routes between the intruders and the destinations are selected using AODV and DSR protocols. In figure 6(a) and figure 6(b), we plot the ratio between the expected number of IDS active insiders of RP and GGO-DOM as a function of the probability of detection of an attack. The plots are similar to those for networks with static insiders, except that the difference between the number of IDS active insiders of RP and GGO-DOM is little lower than that between RP and the optimal algorithm. This is because GGO-DOM selects the IDS active insiders from those selected by GO-DOM, which allows greater overlap among the coverage areas of the selected insiders than the optimal algorithm. The performance difference between RP and GGO-DOM can be explained similarly as that between RP and the optimal algorithm. We draw similar conclusions.

We now investigate the number of IDS active insiders selected by the optimal algorithm and GGO-DOM for high detection probability. The simulation parameters are the same as described in the previous paragraph, except that the insiders are static here. In figure 6(c) and figure 6(d) we plot the probabilities of detection of attacks for these algorithms as functions of the expected number of IDS active insiders. The figures show that both algorithms attain probability of detection 0.9 and 1 when only 15% and 25% of the insiders execute the IDS respectively. Thus, high probabilities of detection are obtained even when only a modest fraction of the insiders operate in promiscuous mode. In most ad hoc networks, at least a small number of insiders have significant energy. Thus, even for high detection probability, it would be sufficient to execute the IDS only in these insiders.

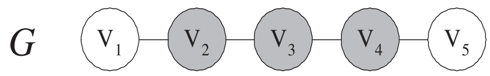


Fig. 7. The shaded insiders are IDS incapable. Thus, only v_1, v_5 may be IDS active. Here, v_3 is a removal insider.

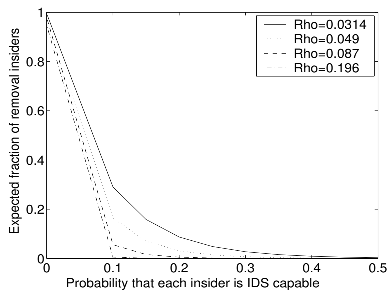


Fig. 8. We plot the expected fraction of removal insiders as a function of φ for different values of ρ.

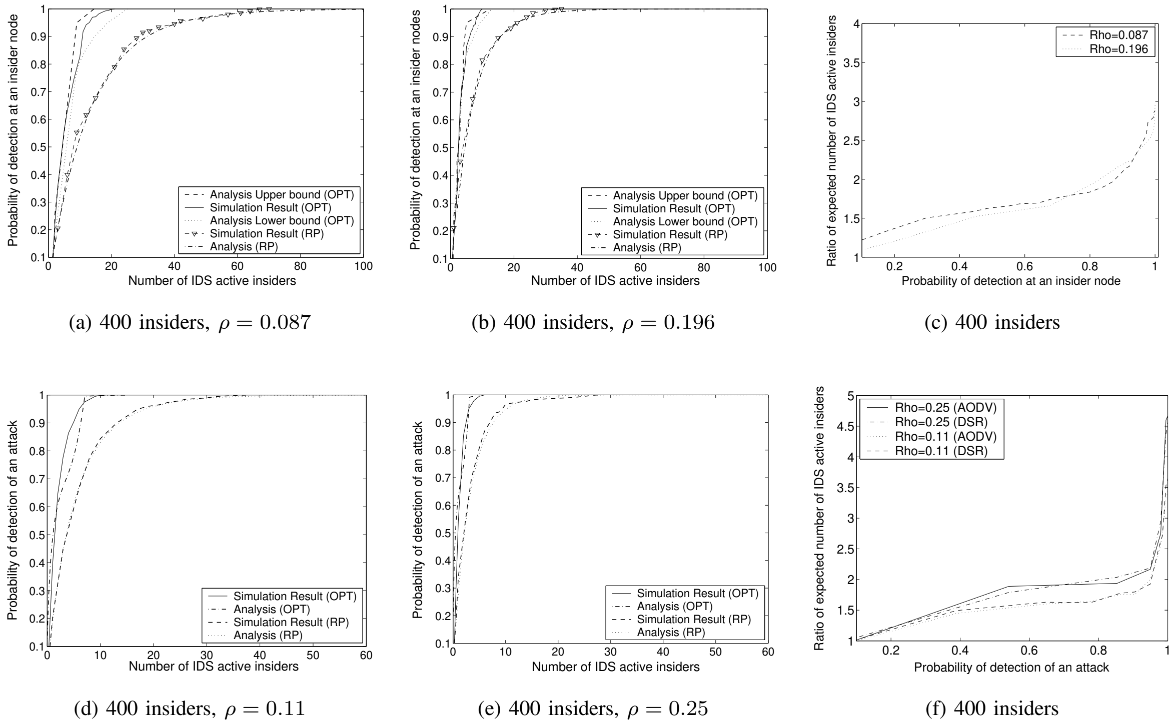
We finally discuss how the presence of IDS incapable insiders limit the performance of the optimal algorithm. When some insiders are IDS incapable, it may not be possible to have the IDS active insiders cover all insiders even when $n = N$. The insiders that are not covered by any IDS capable insider are denoted as "removal insiders" (Figure 7). Specifically, IDS active insiders will not cover the "removal insiders."

Lemma 2: Let $n = N$. Then the optimal algorithm selects the IDS active insiders such that they cover all insiders other than the removal insiders.

Thus, irrespective of the resource used in the detection process, the bad packets that traverse only the removal insiders and are generated by intruders not covered by IDS active insiders will not be detected. Consider a network with N insiders uniformly distributed in a square of area A. Let each insider cover ρ fraction of the total area, and be IDS capable w.p. φ. Let $Z(N, \varphi, \rho)$ be the number of removal insiders in this network. We now quantify $EZ(N, \varphi, \rho)$.

Theorem 7: $EZ(N, \varphi, \rho)/N = 1 - P_D^{\text{RP}}(N, \varphi, \rho)$.

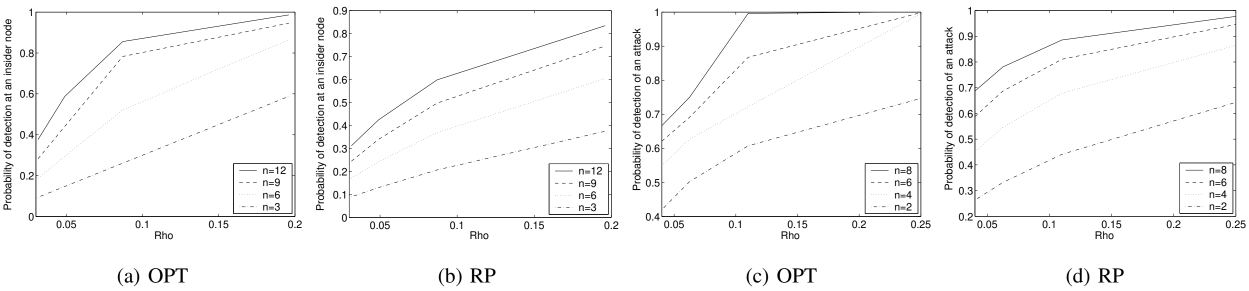
We first present the intuition behind the result. Now, $EZ(N, \varphi, \rho)/N$ is the probability that an insider is a removal insider which equals the probability that all its neighbors are IDS incapable. Also, $1 - P_D^{\text{RP}}(N, \varphi, \rho)$ is the probability that a bad packet transmitted by an insider is not detected under RP in the ETICUS(N, ρ) model, which happens when all neighbors of the insider are IDS inactive. Note that each



(a) 400 insiders, $\rho = 0.087$ (b) 400 insiders, $\rho = 0.196$ (c) 400 insiders

(d) 400 insiders, $\rho = 0.11$ (e) 400 insiders, $\rho = 0.25$ (f) 400 insiders

Fig. 4. In figures (a), (b), (d) and (e), we plot the probabilities of detection as functions of the number of IDS active insiders for the optimal algorithm (OPT) and RP. We obtain the data from the simulation and the analysis. In figures (c) and (f), we plot the ratio of the expected number of IDS active insiders for RP and OPT as a function of the probability of detection for different values of ρ. In figures (a), (b) and (c), we consider probability of detection at a uniformly selected insider. In figures (d), (e) and (f), we consider probability of detection of an attack when packets traverse multiple hops. All insiders are static.



(a) OPT (b) RP (c) OPT (d) RP

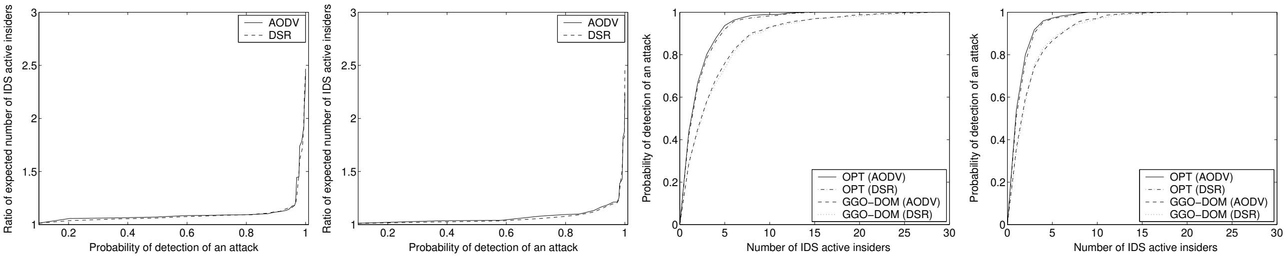
Fig. 5. We plot the probabilities of detection as functions of ρ at different values of n for the optimal algorithm (OPT) and RP. In figures (a) and (b), we consider probability of detection at a uniformly selected insider. In figures (c) and (d), we consider probability of detection of an attack when packets traverse multiple hops. All insiders are static.

insider is IDS incapable in the former case and IDS inactive in the latter case with the same probability $(1 - \varphi)$. The result follows.

Theorems 2 and 7 show that the expected fraction of removal insiders is a monotonically decreasing function of φ and ρ. This is intuitive as with increase in ρ each insider is likely to have larger number of neighbors and thus more likely to have at least one IDS capable neighbor. In Figure 8 we plot the expected fraction of removal insiders as specified in Theorem 7 for several different values of φ and ρ. We observe that even when each insider is IDS capable w.p. only 0.3 this expected fraction is less than 2.3%. Thus the existence of IDS incapable insiders would not significantly decrease the probability of detection.

V. Related Work

Ko *et al.* describe the challenges faced by conventional intrusion detection mechanisms when used in ad hoc networks [11]. We now describe some related work in placing the detection modules which is our focus. Ramanujam *et al.* [18] advocate the use of firewalls on every node with the firewalls being configured to contain the list of allowable packet flows. Like us, they require intermediate nodes to eavesdrop passively. Zhang *et al.* [29] also present a distributed intrusion



(a) $\rho = 0.087$ (b) $\rho = 0.196$ (c) $\rho = 0.087$ (d) $\rho = 0.196$

Fig. 6. We consider topologies with 100 mobile insiders, and 5 mobile intruders attacking 5 destinations. We consider both AODV and DSR routing protocols. In figures a) and b), we plot the ratio of the expected number of IDS active insiders of RP and GGO-DOM as a function of the probability of detection of an attack when packets traverse multiple hops. In figures c) and d), we plot the probability of detection of the optimal algorithm and GGO-DOM as a function of the number of IDS active insiders.

detection and response framework for mobile ad hoc networks, where every node executes the IDS and responds to intrusion. They assume that the nodes cooperate. The disadvantage of both these schemes is that they consume significant energy and computational resource due to involvement of every node in the detection scheme. We present algorithms that maximize the detection rate while minimizing the resource consumption.

We now briefly describe a few other detection schemes that do not consider placement of IDS. Marti *et al.* [14] propose a cooperative routing scheme for avoiding transmitting packets through misbehaving nodes. Nodes promiscuously monitor traffic and cooperate so as to detect and report misbehavior to other nodes. Michiardi *et al.* [16] present the CORE mechanism in which reputation is used to enforce cooperation among nodes and prevent denial of service attacks. Buchegger *et al.* [20] propose the CONFIDANT scheme in which a node monitors its neighborhood to detect intrusion. When a node detects intrusion, it transmits alarm messages to other nodes in its friends list. Rao *et al.* [19] propose to detect intruders by observing node behavior. They propose to estimate the congestion at intermediate nodes and decide if the intermediate node is not forwarding packets at the desired rate because of congestion or because of malicious behavior.

We now distinguish the intrusion detection problem from the related coverage problem in sensor networks [12], [21], [28]. The coverage problem in sensor networks needs coverage of the area under consideration, while intrusion detection in ad hoc networks requires coverage of nodes that transmit the bad packets. Thus the former needs appropriate deployment of sensors to satisfy coverage requirements, while the latter needs appropriate selection of IDS active nodes given the topology. Furthermore, the results obtained in both areas also differ. We have analyzed the probabilities of detection of the optimal node selection algorithms and heuristics for any given value of the transmission radius r and number of nodes N. To the best of our knowledge only few specific sensor deployment algorithms (e.g., grid deployment, random deployment etc.) have been analyzed in sensor networks; also only asymptotic ($r \rightarrow 0$ and $N \rightarrow \infty$) coverage probabilities are known for these.

VI. Conclusion

We investigate the placement of the intrusion detection software for misuse detection in ad hoc networks with multiple, mobile intruders. We mathematically formulate the problem of maximizing the detection probability subject to consuming no more than a certain amount of resource. We show that computing the optimal solution is NP-hard. Thereafter, we propose two polynomial complexity algorithms, Greedy-MC and MUNEN-MC, that approximate the optimal solution within a constant factor, and prove that they attain the best possible approximation ratio. We develop analytical expressions that quantify the resource consumed by the optimal and approximation algorithms and heuristics at different probabilities of detection. We demonstrate using analysis and simulation that the optimal and approximation algorithms consume much less resource for attaining the same probability of detection as compared to a naive algorithm, RP, that randomly places the IDS. Furthermore, attacks can be detected with high probability while using algorithms that are oblivious to the locations and identities of the intruders and the paths used by them, and while consuming modest amount of resource. For example, even for high detection rates ($90-100\%$), the optimal algorithm requires only a modest fraction of nodes to execute the IDS, which can therefore be those that are not limited in energy. Finally, the framework relies on the assumption that the detector modules are never compromised, which we relax in part II of this sequel [26]. Promising areas of future research are the design and implementation of efficient intrusion recovery mechanisms.

VII. Acknowledgement

The authors would like to thank Prof. Sampath Kannan, University of Pennsylvania, for suggesting the use of hybrid algorithms for proving the performance guarantee for MUNEN-MC.

Appendix

Proof of Theorem 1: Refer to Subsection E of appendix of [26].

We now state Lemma 3 which holds due to uniform distribution of insiders. We prove Theorems 2 and 7 using this lemma.

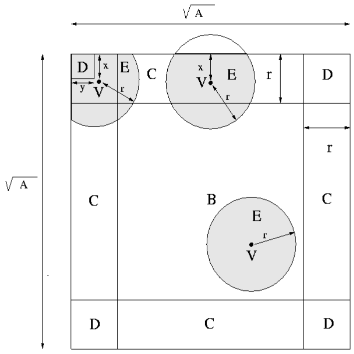


Fig. 9. The shaded areas show the areas E for three different locations of the selected insider V.

Lemma 3: Let N insiders be uniformly distributed in a square of area A. Two nodes are neighbors if and only if the distance between them is less than or equal to r, and $\rho = \pi r^2/A$. Consider an insider V. Each insider u covered by V selects a binary random variable independent of others. Now u selects 1 w.p. t and 0 w.p. $1-t$. Let Q be the event that all of V's neighbors other than V select 0.

$$\begin{aligned}
&\Pr(\mathrm{Q}) \\
&= (1-t\rho)^{N-1}\left(1+\frac{4\rho}{\pi}-4\sqrt{\frac{\rho}{\pi}}\right) \\
&\quad+\left(4\sqrt{\frac{\rho}{\pi}}-8\frac{\rho}{\pi}\right)\times \\
&\quad\int_0^1\left(1-t\rho\left(1-\frac{\cos^{-1}(x)}{\pi}+\frac{x}{\pi}\sqrt{1-x^2}\right)\right)^{N-1}dx \\
&\quad+\frac{4\rho}{\pi}\int_0^1\int_0^1\left(1-t\rho g(x,y)\right)^{N-1}dxdy.
\end{aligned}$$

Proof: Refer to Figure 9. Let R_J denote the event that the uniformly selected insider V is in area J, where $J \in \{B, C, D\}$. Now, $\Pr(Q) = \sum_{J\in\{B,C,D\}} \Pr(R_J)\Pr(Q|J)$, where $\Pr(Q|J)$ is the conditional probability of the event Q given J. Now, since V is selected uniformly among all insiders and the insiders are uniformly distributed in area A, $\Pr(R_J) =$ Area of J/A. Thus,

$$\Pr(R_J) = \begin{cases} 1+4\rho/\pi-4\sqrt{\frac{\rho}{\pi}} & J=B \\ 4\sqrt{\frac{\rho}{\pi}}-8\frac{\rho}{\pi} & J=C \\ 4\rho/\pi & J=D. \end{cases} \quad (5)$$

Now, we compute $\Pr(Q|J)$. Note that Q occurs if each of the $N-1$ insiders other than V are either not V's neighbor or selects 0. Let E be the intersection of the square and the circle with radius r and center at V's location. Any given insider is V's neighbor w.p. area of E/A and if it is V's neighbor it selects 1 w.p. t. Thus $\Pr(Q|J) = (1-t\times$ area of $E/A)^{N-1}$. Now, when $J = B$ area of $E = \pi r^2$.

$$\text{Thus, } \Pr(Q|B) = (1-t\rho)^{N-1}. \quad (6)$$

When $J = C$ area of E is $\rho A\left(1-\frac{\cos^{-1}(x)}{\pi}+\frac{x}{\pi}\sqrt{1-x^2}\right)$ where random variable x specifies V's location in C. Now, random variable x is uniformly distributed in $[0,1]$. Thus,

$$\begin{aligned}
&\Pr(Q|C) \\
&= \int_0^1\left(1-t\rho\left(1-\frac{\cos^{-1}(x)}{\pi}+\frac{x}{\pi}\sqrt{1-x^2}\right)\right)^{N-1}dx.
\end{aligned}$$

When $J = D$ area of E is $\rho A g(x,y)$ where random variables x and y specify V's location in D. Now, random variables x and y are independent and uniformly distributed in $[0,1]$ each.

$$\text{Thus, } \Pr(Q|D) = \int_0^1\int_0^1\left(1-t\rho g(x,y)\right)^{N-1}dxdy. \quad (7)$$

The result follows using (5) to (7). ■

Proof of Theorem 2: Let insider V relay the bad packets. Now, the packets are not detected if V is not IDS active and no other insider covered by V is IDS active. These are independent events. The first happens w.p. $1-q$. Let the second event be denoted as W. Thus, $P_D^{\mathrm{RP}}(N,q,\rho) = 1-(1-q)\Pr(W)$. Under RP, each insider is IDS active w.p. q independent of whether other insiders are IDS active. Thus, $\Pr(W)$ is given by Pr (Q) in Lemma 3 with $t = q$. The result follows.

Proof of Theorem 3: Let the desired probability of detection be P. Then $P \leq P_D^{\mathrm{OPT}}(N,n,\rho) = \frac{S}{N}$ where S is the number of insiders covered by IDS active insiders selected by the optimal algorithm. The last equality holds because the insider that relays the bad packets is uniformly selected. Thus, $S \geq \lceil N\times P\rceil$. Now, let l insiders be IDS active under the optimal selection algorithm where $l \leq \lceil N\times P\rceil$. Then these IDS active insiders must cover at least $\lceil N\times P\rceil - l$ additional insiders. This can happen only when there exists at least one set of l insiders that cover $\lceil N\times P\rceil - l$ or more insiders where $l \leq \lceil N\times P\rceil$. Let this event be denoted as I. Now let $\binom{N}{l}B\left(N,(l\rho)_-,\lceil N\times P\rceil - l\right) < \epsilon$. We show that $\Pr(I) < \epsilon$ Thus, w.p. at least $1-\epsilon$ at least $l+1$ IDS active insiders are required to attain $P_D^{\mathrm{OPT}}(N,n,\rho) = P$. This holds for all l, $l \leq \lceil N\times P\rceil$, for which $\binom{N}{l}B\left(N,(l\rho)_-,\lceil N\times P\rceil - l\right) < \epsilon$ and hence for $\max_{l:l\leq\lceil N\times P\rceil}\{l : \binom{N}{l}B\left(N,(l\rho)_-,\lceil N\times P - l\rceil\right) < \epsilon.\}$ The result follows.

We now prove that when $l \leq \lceil N\times P\rceil$, $\binom{N}{l}B\left(N,(l\rho)_-,\lceil N\times P\rceil - l\right) < \epsilon$, then $\Pr(I) < \epsilon$. Let I_T be the event that insiders in a set T cover $\lceil N\times P\rceil - l$ or more insiders. Now, $I = \cup_{|T|=l} I_T$. Using union bound,

$$\begin{aligned}
\Pr(I) &\leq \sum_{|T|=l}\Pr(I_T) \\
&= \binom{N}{l}\Pr(I_T) \text{ for a given } T \text{ such that } |T| = l \\
&\leq \binom{N}{l}B\left(N,(l\rho)_-,\lceil N\times P\rceil - l\right) \quad (8) \\
&< \epsilon.
\end{aligned}$$

Now (8) holds since l insiders together cover at most $(l\rho)_-$ fraction of the total area, and since insiders are uniformly distributed, number of insiders in $(l\rho)_-$ fraction of the total area is a binomial random variable with parameters $N, (l\rho)_-$ ($(l\rho)_-$ is the success probability of the binomial distribution). Thus $\Pr(I_T)$ for any T with cardinality l is the tail probability of the above binomial distribution. The result follows.

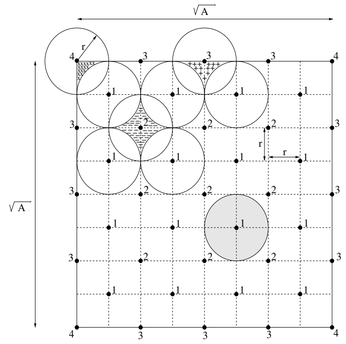


Fig. 10. The figure illustrates an algorithm for selecting IDS active insiders in an area where every point is an insider. The algorithm would execute IDS in insiders at the positions marked $1, 2, 3, 4$. The circles indicate the coverage areas of the insiders that are currently executing the IDS.

Proof of Theorem 4: The bad packets are detected if and only if the selected insider, V, is the neighbor of an IDS active insider. Thus since V is selected uniformly and every point in the square is an insider, $P_D^{\text{OPT}}(n,\rho)$ equals the fraction of the total area covered by IDS active insiders under the optimal algorithm. Thus, $P_D^{\text{OPT}}(n,\rho) \le n\rho$. The optimal algorithm will select IDS active insiders so as to maximize the covered area. We propose a specific coverage process, and thereby obtain a lower bound for $P_D^{\text{OPT}}(n,\rho)$. Refer to Figure 10. If n insiders are selected at positions marked '1' for executing the IDS, each insider covers an additional ρ fraction of the total area (shaded area), and n insiders together cover $n\rho$ fraction of the total area. Since $\sqrt{\pi/\rho}$ is an even integer, there are $\pi/4\rho$ such positions. Thus, for $n \le \pi/4\rho$, $P_D^{\text{OPT}}(n,\rho) = n\rho$. For $\frac{\pi}{4\rho} < n \le \frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1$, insiders at positions marked '2' are selected, and then each additional insider covers an additional area marked '$-$' which is $\rho(4-\pi)/\pi$ fraction of the total area. Thus n insiders cover $\frac{\pi}{4} + (n - \frac{\pi}{4\rho})\frac{\rho(4-\pi)}{\pi}$ fraction of the total area. Thus, for $\frac{\pi}{4\rho} < n \le \frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1$, $P_D^{\text{OPT}}(n,\rho) \ge \frac{\pi}{4} + (n - \frac{\pi}{4\rho})\frac{\rho(4-\pi)}{\pi}$. For $\frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1 < n \le \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3$, insiders at positions marked '3' are selected. Each additional insider covers an additional area marked '$+$' which is $\rho(4-\pi)/2\pi$ fraction of the total area. Thus, for $\frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1 < n \le \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3$, n insiders cover a fraction $1 + \left(n - (\sqrt{\frac{\pi}{\rho}} + \frac{\pi}{2\rho} - 1)\right)\frac{\rho(4-\pi)}{2\pi}$ of the total area. For $n > \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3$, insiders at positions marked '4' are selected. Each additional insider covers an area marked '$\times$' which is $\rho(4-\pi)/4\pi$ fraction of the total area. Thus, for $n > \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3$, n insiders cover $1 + \left(n - (\sqrt{\frac{\pi}{\rho}} + 1 + \frac{\pi}{2\rho})\right)\frac{\rho(4-\pi)}{4\pi}$ fraction of the total area. These justify the lower bounds for $P_D^{\text{OPT}}(n,\rho)$ in these regions.

Proof of Theorem 5: Now we assume that the intruder (I) and its destination (D) are uniformly distributed in a circle of radius R. Thus the distance between them is a random variable L with distribution $f_L(l)$, where $f_L(l) = 4l/\pi R^2 \cos^{-1}(l/2R) - 2l^2/\pi R^3\sqrt{1-(l/2R)^2}$ (p. 129, [22]).

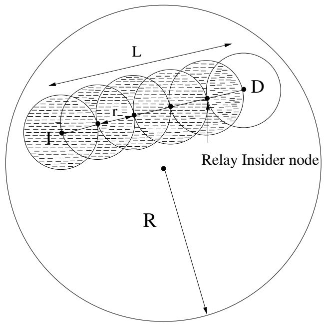


Fig. 11. The figure shows the intruder I, I's target D and relay insiders. The area marked '-' is the total coverage area.

We assume that the path between the intruder and its destination constitutes a straight line. We ignore edge effects, i.e., we assume that irrespective of a node's position, it can have neighboring nodes in a circle of radius r around it. If the distance between the intruder and its destination is less than or equal to r, then there is no relay insider and the attack is detected if there is at least one IDS active insider in the intruder's coverage area which is πr^2. If the distance L between the intruder and its destination exceeds r, then the attack is detected if there is at least one IDS active insider in the coverage areas of the intruder and the relay insiders. This coverage area is $\lceil L/r \rceil(\pi - 1.228)r^2 + 1.228r^2$ (Figure 11). We denote the total coverage area of the intruder and the relay insiders (if the path has relay insiders) by a function $S(L)$ of the distance L between the intruder and its destination. Now, if $L = l$ the coverage area has at least one IDS active insider with probability $1 - (1-q)^{\lceil l/r-1 \rceil}\left(1 - qS(l)/A\right)^{N - \lceil l/r-1 \rceil}$. Thus, the probability of detection of an attack is $1 - \int_0^R (1-q)^{\lceil l/r-1 \rceil}\left(1 - qS(l)/A\right)^{N-\lceil l/r-1 \rceil} f_L(l)dl$. Substituting the values of $S(l)$ and $f_L(l)$ and substituting $l/2R$ with z, r/R with $\sqrt{\rho}$ and appropriately changing the limits of the integration we observe that the above probability equals the right hand side expression in Theorem 5. The result follows. We use the approximation sign, because we have ignored edge effects.

Proof of Theorem 6: Refer to technical report [25].

Proof of Lemma 2: When $n = N$, then all IDS capable insiders can become IDS active. The optimal algorithm selects as many IDS active insiders as required to cover the maximum possible number of insiders. Clearly, a removal insider can not be covered by an IDS active insider. If all the IDS capable insiders execute IDS, every insider that is not a removal insider is covered by an IDS active insider, since every such insider has at least one IDS capable neighbor. The result follows.

Proof of Theorem 7: Let random variable I_i equal 1 if the i^{th} insider is a removal insider and 0 otherwise. Clearly, $Z(N,\varphi,\rho) = \sum_{i=1}^{N} I_i$, and $\Pr(\mathrm{I_i}) = \Pr(\mathrm{I_j})$ for all i,j. Thus, $EZ(N,\varphi,\rho)/N = \Pr(\mathrm{I_1})$. An insider is a removal insider if it is not IDS capable and no other insider in its neighborhood is IDS capable. These are independent events. The first happens w.p. $1-\varphi$. Let the second event be denoted by W. Thus, $\Pr(\mathrm{I_1}) = (1-\varphi)\Pr(\mathrm{W})$. Since each insider is IDS capable w.p. φ independent of others, $\Pr(W)$ is given by Pr (Q) in Lemma 3 with $t = \varphi$. The result follows from appropriate substitution and Lemma 3.

REFERENCES

[1] http://www.esoft.com/products/instagatesoftpaks1.cfm. *Website*.

[2] http://www.microsoft.com/technet/security/bulletin/ms00-066.mspx. *Website*.

[3] J. Beale, A. R. Baker, B. Caswell, and M. Poor. *Snort 2.1 Intrusion Detection*. Syngress, 2nd edition, 2004.

[4] P. Bhagwat, B. Raman, and D. Sanghi. Turning 802.11 inside-out. *ACM SIGCOMM Computer Communication Review*, 34(1):33–38, Jan 2004.

[5] S. Capkun, M. Hamdi, and J. P. Hubaux. Gps-free positioning in mobile ad hoc networks. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34)*, volume 9, pages 3,481–3,490, 2001.

[6] W. Cheswic and W. Bellovin. *Firewalls and Internet Security*. Addison Wesley, 1999.

[7] Eric Cole. *Hackers Beware*. New Riding Publishing, 2001.

[8] D. Denning. An intrusion detection model. In *IEEE Transactions on Software Engineering*, volume SE-13, pages 222–232, Feb. 2001.

[9] S. Garfinkel and G. Spafford. *Practical UNIX and Internet Security*. O'Reilly and Associates, 2nd edition, 1996.

[10] D. Hochbaum. *Approximation Algorithms for NP-Hard Problems*. Thomson Learning, 1996.

[11] C. Ko, P. Brutch, J. Rowe, G. Tsafnat, and K. Levitt. System health and intrusion monitoring using a hierarchy of constraints. In *4th International Symposium, Recent Advances in Intrusion Detection*, pages 190–204, Oct. 2001.

[12] S. Kumar, T. Lai, and J. Balogh. On k-coverage in a mostly sleeping sensor network. In *Proceedings of ACM Mobicom*, pages 144–158, Sep 2004.

[13] H. Luo, R. Ramjee, P. Sinha, L. Li, and S. Lu. Ucan: A unified cellular and ad-hoc network architecture. In *Proceedings of ACM Mobicom*, pages 353–367, Sep 2003.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of ACM Mobicom*, pages 255–265, Aug 2000.

[15] John McHugh. Intrusion and intrusion detection. *International Journal of Information Security*, 1(1):14–35, 2001.

[16] P. Michiardi and R. Molva. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Comminication and Multimedia Security Conference*, pages 107–121, Portoroz, Slovenia, Sep 2002.

[17] David Wagner Nikita Borisov, Ian Goldberg. Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of ACM Mobicom*, pages 180–189, Jul 2001.

[18] R. Ramanujan, S. Kudige, T. Nguyen, S. Takkella, and F. Adelstein. Intrusion-resistant ad hoc wireless networks. In *Proceedings of MILCOM*, volume 2, pages 890–894, Oct 2002.

[19] R. Rao and G. Kesidis. Detecting of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited. In *Proceedings of IEEE Globecom*, pages 2,957–2,961, Dec 2003.

[20] J.Y.L. Boudec S. Buchegger. Performance analysis of the confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, pages 226–236, Jun 2002.

[21] S. Shakkottai, R. Srikant, and N. Shroff. Unreliable sensor grids: Coverage, connectivity and diameter. In *Proceedings of IEEE Infocom*, volume 2, pages 1073–1083, Apr 2003.

[22] H. Solomon. *Geometric Probability*. Society for Industrial and applied mathematics, 1978.

[23] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. Stream control transmission protocol. *RFC 2960*, Oct. 2000.

[24] D. Subhadrabandhu, F. Anjum, S. Kannan, and S. Sarkar. Domination and coverage guarantees through distributed computation. In *Proceedings of 43rd Annual Allerton Conference on Communication, Control, and Computing*, Champaign, IL, Sep. 2005.

[25] D. Subhadrabandhu, S. Sarkar, and F. Anjum. Efficacy of misuse detection in adhoc networks. Technical report, University of Pennsylvania Technical Report, June 2004.

[26] D. Subhadrabandhu, S. Sarkar, and F. Anjum. A framework for misuse detection in ad hoc networks - part ii. In *IEEE Journal on Selected Areas in Communications Special Issue on Security in Wireless Ad Hoc Networks*, 2006.

[27] S. Verblunsky. On the least number of unit circles which can cover a square. In *Journal of the London Mathematical Society*, volume 24, pages 164–170, 1949.

[28] H. Zhang and J. Hou. On deriving the upper bound of alpha-lifetime for large sensor networks. *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, pages 121–132, May 2004.

[29] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of ACM Mobicom*, pages 275–283, Aug 2000.

PLACE PHOTO HERE

Dhanant Subhadrabandhu received the B.Eng. (Hons.) degree in Electrical Engineering from the King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand in 1994. He received the M.S. degree in Telecommunications Engineering from Columbia University, New York, in 1997. He is currently a Ph.D. Candidate in Electrical and Systems Engineering at the University of Pennsylvania, Philadelphia. His research interests are in resource allocation and security issues in wireless networks and distributed systems and algorithms.

PLACE PHOTO HERE

Saswati Sarkar (S'98, M'00) received Phd in Electrical and Computer Engineering from University of Maryland, College Park in 2000. She is currently an Assistant Professor in the department of Electrical and Systems Engineering in University of Pennsylvania. Her research interests are in resource allocation and performance analysis in communication networks. She received a National Science Foundation Faculty Early Career Development Award in 2003. She has been an associate editor of IEEE Transaction on Wireless Communications from 2001.

PLACE PHOTO HERE

Farooq Anjum received the Ph.D. degree from the University of Maryland, College Park in 1999. He is a Senior Scientist at Telcordia Technologies. He is an adjunct professor at University of Pennsylvania (UPenn), Philadelphia and at Stevens Institute of Technology, Hoboken. He has been a member of technical program committees and organizing committees of several leading conferences in networking and security.