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

Dhanant Subhadrabandhu, Saswati Sarkar , Farooq Anjum

***Abstract*— We focus on detecting intrusions in ad hoc networks using the misuse detection technique. We allow for detection modules that periodically stop functioning due to operational failure or compromise by intruders. Combining theories of stochastic coverage processes and approximation algorithms, we develop a framework to counter failure of detection modules while minimizing the resource consumption. We show that the selection of the optimal set of nodes for executing the detection modules is an NP-hard problem. We present a distributed polynomial complexity selection algorithm that attains the best possible approximation ratio. We next consider a simple heuristic selection strategy that allows for seamless operation in time varying topologies. We obtain analytical expressions to quantify the tradeoffs between the resource consumption and detection rates attained by these algorithms. Using analysis and simulation, we identify the appropriate algorithms for different failure rates, resource limitation and required detection rates.**

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

I. INTRODUCTION

We consider ad hoc networks that consist of two classes of nodes: (i) insider nodes who both communicate using the network and perform network tasks like relaying packets, discovering routes, monitoring the network, securing communication, etc. and (ii) outsider nodes who only communicate using the network. Such networks are likely to be widely used in several future applications of practical importance, e.g., disaster recovery operations, battlefields, communication in remote terrains like reservations, rural areas, events like superbowl matches, etc. [6]. An outsider node may wish to deliver malicious (*bad*) packets to a target destination resulting in malfunction or failure of the target. Such an outsider node is referred to as an intruder, and the corresponding event as intrusion. We focus on detecting intrusions using misuse based schemes.

We assume that insiders do not attempt intrusions and consider the following framework for detecting intrusions. Some selected insiders receive in promiscuous mode packets transmitted in their neighborhoods and subsequently analyze them using Intrusion Detection Software (IDS) modules [6]. If the analysis determines that the transmitted traffic contains abnormal packets or "signatures" of attacks, then intrusion is detected. The detection rate and the system resource consumed in detection depend on appropriate selection of these "IDS active" insiders. In Part I of this sequel, we have proposed a framework to select the IDS active insiders so as to maximize the detection rate subject to limiting the resource consumption [6]. This framework relies on the assumption that insiders always detect signatures of the attacks, if any, in the packets transmitted in their neighborhoods. In practice, however insiders periodically stop functioning because of operational failure, power saving operations, compromise by hostile agents like hackers, malicious users etc. We now develop a framework to detect intrusions using unreliable insiders.

We describe the system model in Section II. We mathematically model the problem of countering the failure of IDS active insider nodes while consuming the minimum possible resources (Section III). We prove that optimally selecting the insiders that would sniff and analyze packets is an NP-hard problem. Then, we present a polynomial complexity distributed approximation algorithm, MUNEN (Maximum Unsatisfied Neighbors in Extended Neighborhood) and prove that it attains the best possible approximation ratio. MUNEN only requires local information and limited message exchanges and hence can be deployed in networks without any central control. MUNEN however requires recomputation every time the network topology changes. We subsequently consider a simple randomized selection algorithm, RP (Random placement), that ensures seamless operation in time varying topologies.

We obtain analytical expressions that quantify the detection rates of different algorithms for any given resource availability and the probability of failure (Section IV). Our analysis and simulations reveal that when the probability of failure is moderate and high detection rates are required, then for attaining the same detection rate, the approximately optimal MUNEN consumes significantly lower resource as compared to the simple heuristic RP. Thus, MUNEN must be deployed in this case. But, when these conditions do not hold, RP attains near-optimal performance, and should be preferred.

Finally, we investigate statistical detection processes in which each insider node decides whether there is an attack based on an analysis of some sampled packets (Section V). Clearly, the resource consumption and the detection rate increase with an increase in the sampling frequency. Using the fault model, we obtain a framework to determine for each algorithm the minimum sampling frequency required for a given detection rate. Required detection rates can be attained either by executing IDS in large number of insider nodes which sample traffic at a low rate or by executing IDS in few insider nodes which sample traffic at a high rate. For different algorithms, we determine which option minimizes the resource consumption for attaining a given detection rate — the answers turn out

D. Subhadrabandhu and S. Sarkar are at the Electrical and Systems Engineering Department of the University of Pennsylvania. F. Anjum is at Telcordia Technologies.
The contribution of S. Sarkar was in part supported by the National Science Foundation under grants ANI-0106984, NCR-0238340 and CNS-0435306.
Parts of this paper have been presented at 43rd Annual Allerton Conference on Communication, Control, and Computing, 2005, Monticello, IL.

Notation	Definition
V	Set of insiders
N	Number of insiders
V'	Set of IDS capable insiders
n	Number of IDS active insiders
q	Probability that an IDS capable insider executes the IDS under RP
ρ	The fraction of total area covered by a node
α	Probability of changing state from OI to FI
p	Steady state probability that an insider has failed
M	Number of packets constituting an attack
k	Minimum number of IDS active neighbors of an insider
f	Probability that an IDS active insider samples a packet
$\mathcal{E}$	Energy consumption

TABLE I
NOTATION TABLE

to be significantly different for different algorithms. We prove the analytical results in the appendix, and summarize frequently used symbols in Table I.

II. Threat Model

The system model we adopt is similar to that in Part I of the sequel (Section 2, [6]), except for an additional assumption which requires that the path between an outsider node and its destination has at least one intermediate insider node. Refer to [5] for mechanisms by which a destination can enforce this assumption. The threat models however differ. In this section, we describe our threat model.

When IDS active insider nodes fail, they do not detect bad packets. This may happen due to software and hardware faults, power saving operations*, if the attacker successfully launches a denial of service (DOS) attack on the insider, if the attack has been designed to evade the insider's IDS module [4], if the insider does not receive the packet due to collisions†, poor transmission quality in wireless links, etc. No node however falsely reports a good packet as bad. We also do not consider other forms of misbehavior of failed insiders, e.g., reordering or replicating data packets. This threat model is referred to as the "fault model."

An operational IDS active insider node detects bad packets. We refer to operational insiders as OI and failed insiders as FI. We assume that the status of an insider changes from FI to OI and vice-versa dynamically, as per a markov process that has states FI, OI and probability α of changing state from OI to FI. The steady state probability that an insider node has failed is p. The states of different insiders are mutually independent‡.

Now, the IDS active insiders must be selected such that even when some of these have failed, the required detection rates are achieved while limiting the resource consumption. Also, the selection of the IDS active insiders must be oblivious towards which nodes are FI. This clearly holds as an insider node does not know that the bad packets are evading the IDS module when the attack has been designed to do so or when it is not receiving packets due to poor transmission quality. It may however know of failures due to power saving operations or DOS attacks. But, it may not be able to locate IDS capable neighbors, and hand over the monitoring job to them before or during failure. This happens particularly during sudden failures.

We assume that each attack consists of M bad packets§ For misuse detection, M can be determined from the signatures of the attacks. *An attack is detected only when at least one IDS active insider analyzes all M packets.* This happens only when at least one IDS active insider receives all M packets while it is OI. Although like in [6] we still assume in the analysis that all packets constituting an attack traverse the same path, this assumption no longer implies that an IDS active insider analyzes all packets constituting an attack if it analyzes one packet in the attack. This happens because the status of an IDS active insider may change from FI to OI or vice-versa during an attack. Thus, unlike in [6], the detection rate, and hence the strategy for selecting the IDS active insiders, depends on M.

III. A Mathematical framework for selecting IDS active insider nodes

Our goal is to ensure that irrespective of the locations of the intruders, destinations and the paths between the intruders and their destinations, each attack is detected with a probability of at least P_{det} which is pre-specified. The challenge is to select the IDS active insiders such that this requirement is satisfied while minimizing the resource consumption. In subsection III-A, we mathematically formulate the detection goal. We obtain an algorithm for optimally selecting the IDS active insiders and analyze the probability of detection of this algorithm. The optimal algorithm is however centralized, and its computation complexity is exponential in N. We prove that the optimal selection problem is NP-hard; thus a polynomial complexity computable optimal solution is not likely to exist.

We show that the optimal selection problem is an instance of the set-multicover problem (pp.$112-116$, [7]). Now, unless $P = NP$, the best possible approximation ratio for the set-multicover problem is $\Omega(\ln N)$¶ (pp.$112-116$, [7]).

*During power saving operations (e.g., during "off" and "sleep" modes), a node can not analyze traffic as it either does not receive packets at all or receives at a very low rate. During these modes of operations, a node however saves significant energy than during active modes (like transmit, receive and idle modes). For example, Orinoco wireless card requires 285 mA in transmit mode, 185mA in receive mode, 9 mA in sleep mode and 0 mA in off mode [3].

†Some collisions happen only due to promiscuous operation. Consider an ad hoc network with 3 insider nodes A, B, C. All insiders are IDS capable. Let both A and C be B's neighbors. But, A and C are not each others neighbors. Let B execute the IDS. If A and C simultaneously relay bad packets to outsider nodes, then B does not receive any packet.

‡Most of our results generalize to when states of different nodes are correlated [5].

§Our results can be generalized to consider a set of attacks each of which contains a different number of packets. See [5] for details.

¶A function $f(N)$ is said to be $\Omega(N)$ ($O(N)$) if there exists a positive constant c such that for all large N $f(N) \geq (\leq) cN$.

Approximation algorithms that approximate the optimal solution of the set-multicover problem within a multiplicative factor of $O(\ln(N))$ already exist. But, till date, all approximation algorithms that are known to provide worst case approximation guarantees ($O(\ln(N))$ or any other meaningful bound) are centralized. In subsection III-B, we present a distributed polynomial complexity computable selection algorithm MUNEN ("Maximum Unsatisfied Neighbors in Extended Neighborhood") that attains the best possible approximation ratio of $O(\ln(N))$. MUNEN selects the IDS active insiders using only local information and simple computations and can therefore be used in large scale networks.

MUNEN is oblivious to the movement of outsiders, but requires re-computation whenever insiders move. In subsection III-C, we consider a simple heuristic selection strategy RP ("Random Placement") that does not have provable approximation bound, but nevertheless does not require such re-computations and is therefore more suitable when insiders move rapidly. We analyze the probability of detection for RP. All the algorithms proposed in this section are oblivious towards locations, identities of the intruders and the paths used by them.

A. Optimal Selection of IDS Active Insider Nodes

An attack is detected only when at least one IDS active insider receives all M packets while it is OI. The probability that any one IDS active insider receives all M packets while it is OI decreases with increase in p. Thus, a desired detection rate may only be attained if the IDS active insiders are selected so that each insider is covered by multiple IDS active insiders. We now determine the coverage requirement for each insider.

First assume that $M = 1$, e.g., a land exploit attack [1] consists of one bad packet. Thus, when an insider node i which is covered by k IDS active insider nodes relays a bad packet, the packet is detected with probability (w.p.) $1 - p^k$[‖]. Now, i may be the only insider in the path between an intruder and its destination. Thus, $1 - p^k$ must not be less than P_{det}. Thus, $k \geq \frac{\ln\left(1-P_{\text{det}}\right)}{\ln(p)}$. If each packet traverses multiple hops before reaching the destination, then each insider node may be covered by fewer IDS active insiders. But, since the paths are not known and change with node mobility, it is necessary to provide the guarantees in the worst case scenario.

Now consider arbitrary M. Since all M packets in an attack traverse the same path, an IDS active insider node detects an attack relayed in its neighborhood w.p. $(1-p)(1-\alpha)^{M-1}$. If an insider node is covered by k IDS active insider nodes, then any attack it relays is detected w.p. $1 - \left(1-(1-p)(1-\alpha)^{M-1}\right)^k$. Thus, the attack is detected w.p. P_{det} only when $k \geq \frac{\ln\left(1-P_{\text{det}}\right)}{\ln(1-(1-p)(1-\alpha)^{M-1})}$.

We now investigate whether the IDS active insiders should be selected so that all the insiders are covered uniformly. In other words, we investigate whether the detection probability is higher when all insiders are covered by the same number of IDS active insiders or when different insiders are covered by different number of IDS active insiders. In the first case the probability of detection does not depend on which insider relays the bad packets. In the latter case, however, an attack will be detected with high probability when bad packets are relayed by some insiders and low probability when bad packets are relayed by other insiders, but the overall probability of detection may be high. We determine whether this is indeed the case.

Let insiders execute IDS such that γ_i fraction of insiders are covered by k_i IDS active insiders, where $\sum_i \gamma_i = 1$. The path between an intruder and its destination may consist of only one insider. Thus, the worst case detection probability is $1 - \sum_i \gamma_i r^{k_i}$, where $r = 1-(1-p)(1-\alpha)^{M-1}$. Using concavity of the function $f(k) = 1 - r^k$ for any non-negative r, one can show that $1 - \sum_i \gamma_i r^{k_i} \leq 1 - r^{\sum_i \gamma_i k_i}$. When $\sum_i \gamma_i k_i$ IDS active insiders cover each insider, (which is possible if $\gamma_i k_i$ is an integer), the probability of detection is $1 - r^{\sum_i \gamma_i k_i}$. Both schemes consume similar amount of resource as the average number of IDS active insiders covering each insider is $\sum_i \gamma_i k_i$ in both cases. Thus *subject to the same resource consumption the probability of detection is maximized when the IDS active insiders are selected so as to equalize the number of IDS active neighbors of each insider node.* If $\sum_i \gamma_i k_i$ is not an integer, then it follows from Lemma 2 in the appendix that equalizing the number of IDS active neighbors of each insider as far as possible increases the probability of detection without increasing the resource consumption. *Thus, we must select the IDS active insiders among the IDS capable insiders such that each insider is covered by at least k IDS active insiders, where* $k = \lceil \frac{\ln\left(1-P_{det}\right)}{\ln(1-(1-p)(1-\alpha)^{M-1})} \rceil$, *while minimizing the number of the IDS active insiders which is the resource consumed in the detection.*

The optimal set of IDS active insiders can be computed by solving an integer linear program, MRRDU_{IP} (minimize resource consumption subject to attaining the required detection probability using unreliable insider nodes). For each insider there exists an integer variable x_i. Now, $x_i = 1$ if i is IDS active, and 0 otherwise. Since every insider must be covered by at least k IDS active insiders, $\sum_{j \in N'_i} x_j \geq k$. The goal of MRRDU_{IP} is to minimize the number of the IDS active insiders, i.e., $\sum_{j \in V} x_j$ subject to these constraints.

(MRRDU_{IP}) Minimize: $\sum_{j \in V} x_j$
subject to
1) $\sum_{j \in N'_i} x_j \geq k, \forall\, i$
2) $x_i \in \{0, 1\}\ \forall\, i\ \in V$.

Note that it may not be possible to select IDS active insiders so as to cover every insider by k IDS active insiders. This happens when an insider node is covered by at most $k-1$ IDS capable insiders (i.e., when $|N'_i| < k$ for some i). Then, MRRDU_{IP} will be infeasible. But, even in this case, MRRDU_{IP} can be slightly modified to ensure feasibility and provide *maximum possible coverage* in the following sense: if an insider has $k-1$ or fewer IDS capable neighbors, all its IDS capable neighbors are IDS active. For this, the constraint in MRRDU_{IP} that $\sum_{j \in N'_i} x_j \geq k$, $\forall\, i$ must be replaced by the constraint that $\sum_{j \in N'_i} x_j \geq \min(k, |N'_i|)$, $\forall\, i$. For simplicity of exposition, henceforth, unless otherwise stated, we assume that $|N'_i| \geq k$

[‖] This happens since each insider is FI w.p. p in the steady state and the selection of the IDS active insiders is oblivious to whether an insider is FI.

for all i. Thus, MRRDU$_{\text{IP}}$ is feasible.

We now analyze the probability of detection attained by the optimal algorithm when n insiders are IDS active. This analysis will quantify the tradeoff between resource consumption and detection probability. When IDS active insiders are selected so as to cover each insider node at least k times where $k = \lceil \frac{\ln(1-P_{\text{det}})}{\ln(1-(1-p)(1-\alpha)^{M-1})} \rceil$, the probability of detection will exceed P_{det} as some insiders will have more than k IDS active neighbors. For example, consider a linear array of insiders A, B, C, D, E. Every insider is a neighbor of its adjacent insiders. If $k = 1$, the optimal algorithm will execute IDS in B and D. Thus, C will have 2 IDS active neighbors. The analysis will allow us to estimate the difference between P_{det} and the achieved probability of detection.

The analysis of the probability of detection of the optimal algorithm is complicated as the number of IDS active neighbors of any insider node depends on the entire topology. We therefore restrict ourselves to the ETICUS(N, ρ) model for the network (Section IV, 3^{rd} paragraph, [6]). Our goal is to compute the probability of detection of an attack when n insiders execute IDS and the bad packets are relayed by a uniformly selected insider ($P_D^{\text{OPT}}(N, n, p, \rho, M)$). We obtain two approximations which we intuitively argue as upper and lower bounds for $P_D^{\text{OPT}}(N, n, p, \rho, M)$ respectively. For obtaining the approximations, we consider the ETICDS(ρ) model (Section IV, after Theorem 3, [6]). We obtain the maximum possible probability of detection $P_D^{\text{OPT}}(n, p, \rho, M)$ in this model. Note that $P_D^{\text{OPT}}(n, p, \rho, M)$ does not depend on N. For large N, $P_D^{\text{OPT}}(N, n, p, \rho, M) \approx P_D^{\text{OPT}}(n, p, \rho, M)$. Computing $P_D^{\text{OPT}}(n, p, \rho, M)$ is again difficult as it requires the characterization of the maximum possible area covered by n discs of area ρ in a unit square, which to the best of our knowledge, is an open problem in mathematics. Asymptotic upper bounds for this maximum possible area is however known [8]. We could however upper and lower bound $P_D^{\text{OPT}}(n, p, \rho, M)$ for any n, ρ, p, M.

Theorem 1: Consider the ETICDS(ρ) model. If $n\rho$ is an integer then,

$$P_D^{\text{OPT}}(n, p, \rho, M) \leq 1 - \left(1 - (1-p)(1-\alpha)^{M-1}\right)^{n\rho}.$$

else,

$$\begin{aligned} &P_D^{\text{OPT}}(n, p, \rho, M) \\ &\leq \; 1 - (\lceil n\rho \rceil - n\rho)\left(1 - (1-p)(1-\alpha)^{M-1}\right)^{\lfloor n\rho \rfloor} \\ &\quad -(n\rho - \lfloor n\rho \rfloor)\left(1 - (1-p)(1-\alpha)^{M-1}\right)^{\lceil n\rho \rceil}. \end{aligned}$$

We intuitively explain this result. Let $n\rho$ be an integer. Clearly, n IDS active insiders cover at most $n\rho$ fraction of the total area. Since each point in the square is an insider, each insider node is covered by at most $n\rho$ IDS active insiders. Then any attack an insider relays is detected w.p. $1 - \left(1 - (1-p)(1-\alpha)^{M-1}\right)^{n\rho}$.

In Theorem 4 in the appendix, we lower bound $P_D^{\text{OPT}}(n, p, \rho, M)$.

Since for large N, $P_D^{\text{OPT}}(N, n, p, \rho, M) \approx P_D^{\text{OPT}}(n, p, \rho, M)$, for large N, Theorems 1 and 4 provide upper and lower bounds for $P_D^{\text{OPT}}(N, n, p, \rho, M)$.

We now examine the complexity of the optimal algorithm. We no longer limit ourselves to the ETICUS(N, ρ) model, and consider arbitrary distributions for insider nodes and arbitrary edge sets. The complexity of solving MRRDU$_{\text{IP}}$ is exponential in N. Furthermore, the following lemma implies that unless $P = NP$ the complexity of solving the optimal selection problem cannot be polynomial in N.

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

Proof: We first describe the set-multicover problem which is well-known to be NP-hard [2]. There exists a set U with elements $\{u_1, \ldots, u_N\}$ and K subsets of U: $U_1, \ldots, U_K$. The goal is to select the minimum number of subsets such that each element belongs to k or more selected subsets. We now show that the set-multicover problem can be solved in polynomial complexity if MRRDU$_{\text{IP}}$ can be solved in polynomial complexity. Now, consider a wireless network with IDS capable insiders $v_1, v_2, \ldots, v_K$ and IDS incapable insiders $u_1, \ldots, u_N$. Let $E = \{(v_i, u_j), 1 \leq i \leq K, u_j \in U_i\} \cup \{(v_i, v_j), 1 \leq i \leq K, 1 \leq j \leq K\} \cup \{(u_i, u_i), 1 \leq i \leq N\}$. Here, $V' = \{v_1, \ldots, v_K\}$, $N_{v_i} = V' \cup U_i$, for each $i \in \{1, \ldots, K\}$. Thus v_i covers all insiders in U_i and no insider in $U \setminus U_i$. Let the coverage requirement be k for each insider. Clearly, any feasible solution for MRRDU$_{\text{IP}}$ selects at least k insiders from V' and no insider from $V \setminus V'$. Thus, for any feasible solution, insiders in V' are covered by at least k IDS active insiders. Thus, the optimal solution for MRRDU$_{\text{IP}}$ is a feasible solution that selects minimum number of insiders from V' subject to ensuring that every insider in U is covered with at least k selected insiders. Thus, the optimal solution for MRRDU$_{\text{IP}}$ provides the optimal solution for the set-multicover problem. ■

B. Distributed Algorithms for Approximating the Optimal Selection within Guaranteeable Approximation Bound

We now consider algorithms for approximating the optimal selection problem. The proof for Lemma 1 demonstrates that the optimal selection problem is an instance of the set-multicover problem. Thus, the best possible approximation ratio** for this selection problem is $\Omega(\ln N)$ (pp.$112 - 116$, [7]). Furthermore, till date, all existing approximation algorithms for the set-multicover problem with worst case approximation guarantees lead to centralized solutions. We design a distributed polynomial complexity approximation algorithm MUNEN that not only attains the best possible approximation ratio of $O(\ln N)$, but also selects the same set of insiders as the best known centralized approximation algorithm for the set-multicover problem, Greedy (pp.$112 - 116$, [7]).

We first adapt Greedy to the selection problem. We first introduce a new notion.

Definition 1: The *k-priority* of an insider node is the number of its neighbors that are covered by fewer than k IDS active insiders.

Greedy iteratively selects the IDS active insiders. In each iteration, it selects an IDS capable insider v that (a) has not been

**The approximation ratio of a node selection algorithm is the ratio between the number of nodes it selects and the number of nodes the optimal algorithm selects.

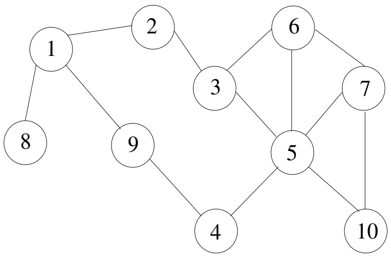


Fig. 1. Let $k = 2$ and let all insider nodes be IDS capable. Greedy selects insiders $5, 1, 3, 9, 7, 8$ in iterations $1, 2, 3, 4, 5, 6$ respectively. MUNEN selects insiders 1 and 5 in the first iteration. Then it selects insiders 3 and 9 in the second and third iterations respectively. Finally, it selects insiders 7 and 8 in the last iteration.

selected yet (b) has positive k-priority and (c) has the maximum k-priority among all IDS capable insiders that have not been selected††. After each selection, every insider in the 2-hop neighborhood of the selected insider recomputes its k-priority.

The selection process terminates when all IDS capable insiders that have not been selected have k-priority 0. Clearly, Greedy requires $|V'|$ or fewer iterations. Thus, Greedy's complexity is $O(|V'|^2)$.

Figure 1 elucidates the operation of Greedy (and MUNEN).

Greedy selects a set of IDS active insiders whose cardinality is at most $\sum_{i=1}^{d}(1/i)$ times that of the optimal set of IDS active insiders, where d is the maximum number of neighbors of an insider (pp.$115-116$, [7]). Now, $\sum_{i=1}^{d}(1/i) = H(d) \leq H(N)$ and $H(N)$ is $O(\ln N)$. Thus, Greedy attains the best possible approximation ratio.

The problem with Greedy is that before the selection of each IDS active insider it needs a network-wide communication to determine which insider has the maximum k-priority in the network. Thus, it is centralized.

We now design a polynomial complexity approximation algorithm, MUNEN that selects the same set of insiders as Greedy, but uses only local information at each insider - MUNEN is therefore distributed.

We now describe MUNEN. We first introduce the following terminologies. Let $h(u, v)$ be the minimum number of hops between insiders u, v. Let $N^2(u)$ be the set of IDS-capable $2-$hop neighbors of u not including u, i.e., $N^2(u) = \{v : v \in V' \setminus \{u\}, h(u, v) \leq 2\}$.

In each iteration an IDS-capable insider u selects itself if

- u has not selected itself already and
- u's k-priority is positive and
- for any other insider v that has not been selected yet and is in $N^2(u)$, either (i) u's k-priority is greater than that of v or (ii) u's k-priority equals that of v and $u < v$.

At the end of each iteration, insiders recompute their k-priorities.

Clearly, MUNEN selects additional IDS active insiders in each iteration until each IDS capable insider that has not been selected has 0 k-priority. It can select at most $|V'|$ insiders. Thus, MUNEN terminates in at most $|V'|$ iterations, and the complexity of the computations at each insider is $O(|V'|^2)$.

††If multiple IDS capable insiders have the maximum k-priority, Greedy selects the one with the least identity among them.

Theorem 2: MUNEN selects the same set of IDS active insiders as Greedy.

Thus, MUNEN attains the best possible approximation ratio as well. We therefore do not consider Greedy any further.

Finally, if $|N_i'| < k$ for some i and therefore it is not possible to select IDS active insiders so as to cover every insider by k IDS active insiders, then MUNEN provides the maximum possible coverage.

C. A Simple Heuristic for Selecting IDS Active Insiders

MUNEN is oblivious to the position of the outsider nodes, and is therefore not affected by their movements. But, it needs to recompute the IDS active set each time an insider node's neighborhood changes due to its or its neighbors' movements. Even though insiders require only local information and limited message exchanges during such computations, frequent execution of these computations may consume significant resource. Thus, MUNEN may not be suitable when the insider nodes move rapidly.

We now consider the naive randomized node selection algorithm RP [6] that does not require any re-computation with movement of either insider or outsider nodes, and does not require any message exchange whatsoever. Recall that in RP every IDS capable insider node executes the IDS with a probability q which can be selected so as to regulate the resource consumed and the detection rate. The disadvantage of RP is that it requires a larger number of IDS active insiders and hence consumes more resource for attaining the same probability of detection as compared to MUNEN.

We compute RP's probability of detection of the bad packets $P_D^{\text{RP}}(N, q, p, \rho, M)$ while being relayed by a uniformly selected insider node. We again restrict ourselves to the ETICUS(N, ρ) model for the network (Section IV, 3^{rd} paragraph, [6]).

First, consider the simple case that $\rho << 1$. In this case, we can ignore the "edge effects," i.e., we assume that each node's coverage area is within the overall area. Now, let an insider B relay packets constituting an attack. Now, B detects the attack if it is IDS active and if it is OI during the transmission of all M packets - these events simultaneously occur w.p. $q(1-p)(1-\alpha)^{M-1}$. Any other insider C detects the attack if it is B's neighbor, if it is IDS active and if it is OI during the transmission of all M packets - these events simultaneously occur w.p. $q\rho(1-p)(1-\alpha)^{M-1}$. The attack is not detected when neither B nor any other insider detects the attack. Since there are $N-1$ insiders in the network other than B, the attack is not detected w.p. $\left(1-q(1-p)(1-\alpha)^{M-1}\right)\left(1-q\rho(1-p)(1-\alpha)^{M-1}\right)^{N-1}$. Thus if $\rho << 1$,

$$P_D^{\text{RP}}(N, q, p, \rho, M) \approx 1 - \left((1-q(1-p)(1-\alpha)^{M-1}\right) \times \left(1-q\rho(1-p)(1-\alpha)^{M-1})^{N-1}\right) \quad (1)$$

For arbitrary ρ, C's detection probability is no longer $q\rho(1-p)(1-\alpha)^{M-1}$ as the probability that C is B's neighbor is less than ρ; thus (1) does not hold. However, the following theorem provides $P_D^{\text{RP}}(N, q, p, \rho, M)$ for arbitrary N, q, p, ρ, M.

Theorem 3: Consider the ETICUS(N, ρ) model.

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

Recall that $g(x, y)$ has been defined in Theorem 2, Section IV [6] as follows.

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

When $\rho << 1$ each of the integrands in (2) becomes approximately equal to 1, and (2) reduces to (1).

In Section IV, we compare the performances of MUNEN and RP, and determine when each may be deployed.

IV. Performance Evaluation

Using analysis and ns2-simulations, we compare the performances of the optimal algorithm, MUNEN and RP for selecting the IDS active insiders. The simulations allow us to investigate the tightness of the analytical bounds and the effect of the factors we did not consider in the analysis, e.g., multihop paths, multiple intruders, movement of intruders etc. We also evaluate the benefits of intelligently selecting the IDS active insiders, and accordingly decide the appropriate selection algorithm for any desired tradeoff between detection efficiency and resource consumption. In our simulations, insiders are static and are distributed as per the ETICUS(N, ρ) model with $N = 400, 100, 80$, $A = 600^2m^2, 400^2m^2$, $\rho = 0.087, 0.1963$ and $p = 0.2, 0.4, 0.6$. Unless otherwise stated, we use $A = 600^2m^2$. In each case, we consider 200 different trials.

We first compare the analytical expressions obtained in Theorems 1, 4, 3 with measurements obtained from simulations. In each trial a single intruder launches an attack consisting of one bad packet ($M = 1$) which a uniformly selected insider relays to an outsider. The probability of detection is measured as the percentage of trials in which the bad packet is detected while being relayed by the uniformly selected insider node. 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 approximate this computation using MUNEN. We proceed as follows. Given n, we compute the maximum k, $k(n)$, such that MUNEN can cover each insider with k or fewer IDS active insiders while selecting n or fewer IDS active insiders. Then, we execute IDS in the insiders selected by MUNEN with $k = k(n)$. Sample computations suggest that MUNEN closely approximates the optimal, and the performance difference is generally much less than the approximation bound presented in Section III-B (Figure 2). In RP the expected number of IDS active nodes is Nq. Thus, for even comparison with the optimal algorithm, we select $q = n/N$.

In Figures 3 (a), (b), (c), (d), (e) and (f), we plot the probabilities of detection measured from simulation and that obtained from the analytical expressions ($P_D^{\mathrm{RP}}(N, n/N, p, \rho, 1)$ obtained from Theorem 3 and the upper and lower bounds for $P_D^{\mathrm{OPT}}(N, n, p, \rho, 1)$ obtained from Theorems 1 and 4 respectively) as functions of the expected number of IDS active insiders, n, for $N = 400$ and different values of ρ and p. These plots demonstrate that the results obtained from the simulation and the analysis match closely for RP. For OPT, as expected, the detection probability measured in the simulation is between the two bounds. The lower bound is closer to the simulation measurements, except for high p ($p = 0.6$). For high p, the upper bound is a better approximation in many cases.

In Figures 3 (g) and (h), we plot the ratio between the expected number of IDS active insiders of RP and MUNEN as a function of the probability of detection. We obtain this ratio from simulation measurements. These figures help us understand the different tradeoffs between probability of detection and resource consumed in the detection process obtained by different algorithms. For high p ($p > 0.5$), RP and MUNEN perform similarly. Now consider low p ($p \leq 0.4$). For high probability of detection, RP requires significantly higher number of IDS active insiders as compared to MUNEN. But, for low probability of detection, RP and MUNEN require similar number of IDS active insiders. For all probabilities of detection, the difference between RP and MUNEN decreases as p increases. Thus, given its low resource consumption, MUNEN should be used when p is low and moderate to high detection probabilities are required. Given its simplicity, RP should be used otherwise. Since MUNEN and OPT perform similarly, the detection probability thresholds for switching between MUNEN and RP can be decided using the analytical expressions for OPT and RP in Theorems 1, 4, 3.

We now explain the difference in performance between MUNEN and RP. Intuitively, MUNEN is expected to perform better than RP because unlike RP it selects insiders such that their coverage areas minimally overlap. But, this happens only at low p. For high p, MUNEN requires a high k and hence selects the IDS active insiders such that each insider is covered by several IDS active insiders. At any time, a random number of insiders in this set are OI and detect packets. Thus, the coverage areas of the OI insiders do not minimally overlap. Therefore, MUNEN and RP behave similarly. Now, consider low p. For both MUNEN and RP, the detection probability increases with increase in the number of IDS active insiders, but by different amounts for different detection probability. Now, for MUNEN the total area covered by the IDS active insiders, and hence the detection probability always increase by similar amounts for equal increase in the number of IDS active insiders. This is because, for low p, MUNEN selects the IDS active insiders such that each insider is covered by few IDS active insiders, and thus their coverage areas minimally overlap. This however does not always hold for RP. Recall that RP selects the IDS active insiders uniformly in the entire set of insiders. Since the insiders are uniformly distributed in the overall area, this is equivalent to selecting the IDS active insiders such that they are uniformly distributed as well. When RP has a low detection probability, its IDS active insiders cover a small area. 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 detection probability, similar to MUNEN, RP selects the IDS active insiders such that their coverage areas minimally overlap. Therefore, RP and MUNEN have similar increase in the coverage area and hence similar increase in the detection probabilities for the same increase in the number of IDS active insiders in this case. When RP has a high detection probability, its 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, for high detection probability, unlike MUNEN, RP selects the IDS active insiders such that their coverage areas significantly overlap. Therefore, compared to MUNEN, RP has much smaller increase in coverage area and hence detection probabilities for the same increase in the number of IDS active insiders in this case. Conversely, at high detection probabilities, for equal increase in detection probabilities, compared to MUNEN, RP needs to execute the IDS in many more insiders.

We now consider networks with 5 intruders and 5 target nodes. Each intruder attacks its designated target, and the path between them is selected as per the AODV protocol and can have several intermediate insider nodes. Like insiders, intruders and their targets are also uniformly distributed in the overall area. Each intruder moves as per the random way point model with a maximum speed of 20 m/s and pause time 10 sec. Here, $\alpha = 0.001$. Each attack consists of 10 packets and is detected if all 10 packets are detected by a single IDS active insider. We measure the probability of detection of attacks as the percentage of attacks that are detected over all trials. In figure 4 we plot the ratio between the expected number of IDS active insiders of RP and MUNEN as a function of the probability of detection of the attack. The trends remain the same as in figures 3 (g) and (h). Thus our conclusions are unchanged.

V. Sampled Detection Processes

We consider a statistical detection process where each of the n IDS active insiders samples the traffic at a predetermined rate f and detects intrusion on the basis of the sampled traffic. The statistical detection process allows each IDS active insider to operate in power saving mode (sleep or off mode) while not sampling and thereby save significant energy[‡‡] and prolong its lifetime.

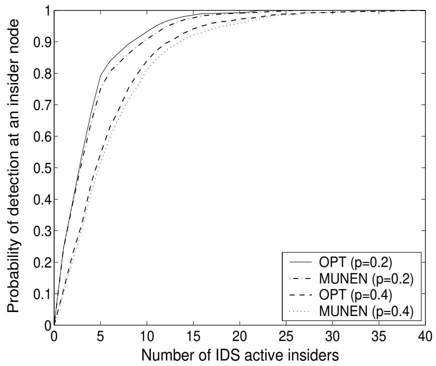


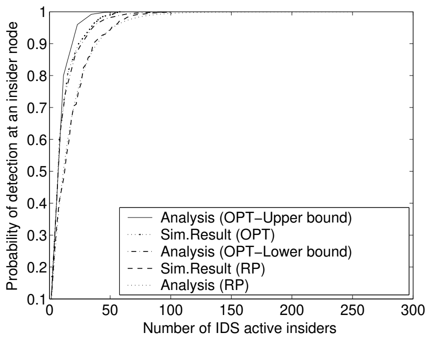
Fig. 2. We consider topologies where a single intruder sends a bad packet through a uniformly selected insider to an outsider. We plot the probability of detection of the bad packet for OPT and MUNEN as functions of the number of IDS active insiders for $N = 80, A = 400^2 m^2, \rho = 0.196$ and different values of p. We obtain the data from simulation.

The energy consumed in detection by each IDS active insider linearly increases with increase in f; we ignore the proportionality constants and assume that this energy is f. The energy consumed by the system in the detection process $\mathcal{E}$ is the sum of the energy consumed by the nodes, i.e., $\mathcal{E} = nf$. We seek to minimize $\mathcal{E} = nf$ by appropriately selecting the system parameters. Clearly, a desired probability of detection can be obtained by selecting a high n and low f or a low n and high f. It is not clear which of the above options minimizes $\mathcal{E}$, and the answer is likely to depend on the algorithm that selects the IDS active insiders. Using our fault model, we develop a framework for computing the optimum tradeoff for different algorithms. *Our goal is to select n and f so as to minimize the energy consumption $\mathcal{E}$ subject to attaining the desired probability of detection.*

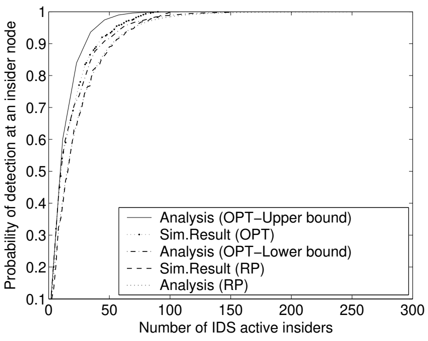
For simplicity, we consider a simple sampling strategy where each IDS active insider node samples each packet w.p. f independent of other packets. We can consider an insider node to be OI when it samples the packet and FI otherwise. Thus each insider is FI w.p. $1 - f$. We assume that each attack consists of one packet that traverses a single insider node. Now, substituting $p = 1 - f$, $M = 1$ and $q = n/N$, Theorems 1 and 4 provide upper and lower bounds for the detection probability of the optimal algorithm ($P_D^{\text{SOPT}}(n, f, \rho)$) and Theorem 3 provides the detection probability of RP ($P_D^{\text{SRP}}(N, n, f, \rho)$) when an IDS active insider samples a packet w.p. f.

$$\begin{aligned}
&P_D^{\text{SRP}}(N, n, f, \rho) \\
&\quad = \quad 1 - (1 - \frac{nf}{N})[(1 - \frac{nf\rho}{N})^{N-1}\left(1 + \frac{4\rho}{\pi} - 4\sqrt{\frac{\rho}{\pi}}\right) \\
&\qquad + \left(4\sqrt{\frac{\rho}{\pi}} - 8\frac{\rho}{\pi}\right)\int_0^1 \left(1 - (\frac{nf\rho}{N})\times\right. \\
&\qquad \left.\left(1 - \frac{\cos^{-1}(x)}{\pi} + \frac{x}{\pi}\sqrt{1 - x^2}\right)\right)^{N-1} dx
\end{aligned}$$

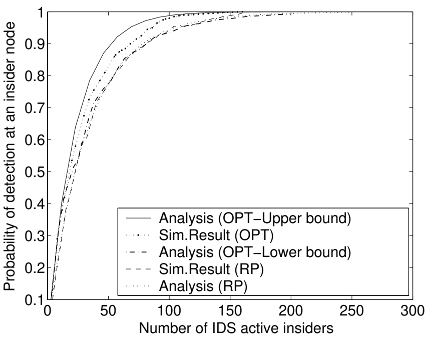
‡‡The statistical detection process also allows an insider to save processor cycles and reduces memory usage. Although we explicitly discuss energy consumption, the analysis applies to other resources as well.



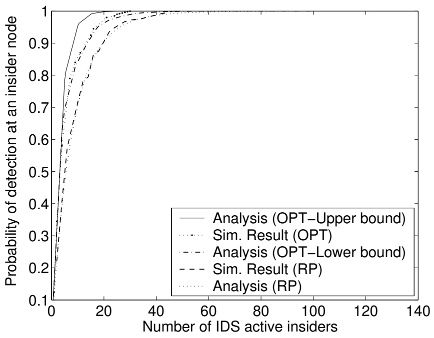
(a) $\rho = 0.087, p = 0.2$



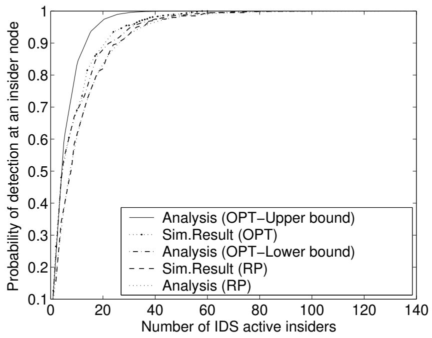
(b) $\rho = 0.087, p = 0.4$



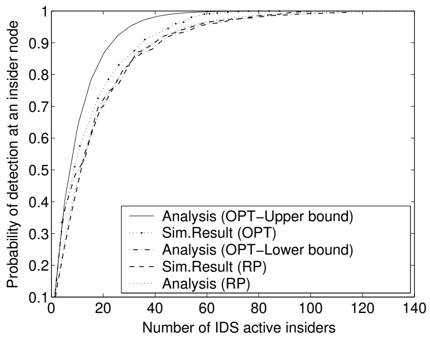
(c) $\rho = 0.087, p = 0.6$



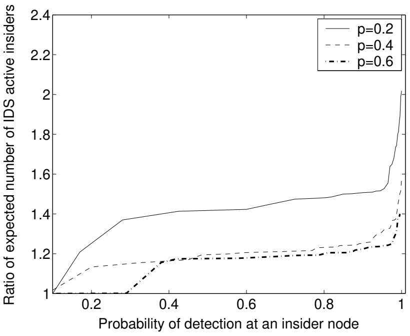
(d) $\rho = 0.196, p = 0.2$



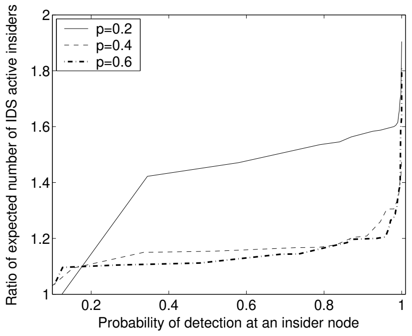
(e) $\rho = 0.196, p = 0.4$



(f) $\rho = 0.196, p = 0.6$



(g) $\rho = 0.087$



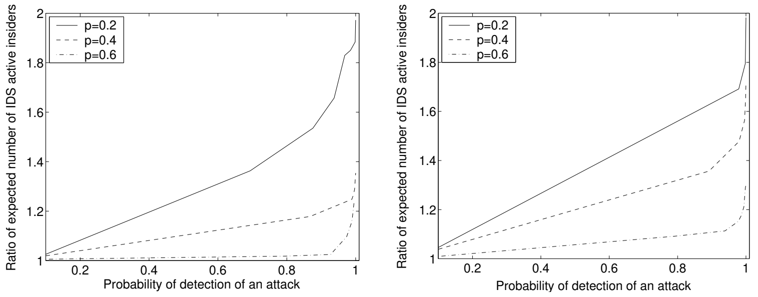
(h) $\rho = 0.196$

Fig. 3. We consider topologies where $N = 400$ and a single intruder sends a bad packet through a uniformly selected insider to an outsider. In figures (a), (b), (c), (d), (e) and (f), we plot the probabilities of detection of the bad packet as functions of the expected number of IDS active insiders for different values of p and ρ for OPT and RP. We plot both probabilities measured from the simulation and obtained from the analysis. In figures (g) and (h), we plot the ratio of the expected number of IDS active insiders of RP and MUNEN as a function of the probability of detection measured from the simulation for different values of p and ρ.

$$+\frac{4\rho}{\pi}\int_0^1\int_0^1\left(1-\frac{nf\rho g(x,y)}{N}\right)^{N-1}dxdy].$$

Thus, $P_D^{\mathrm{SRP}}(N, n, f, \rho)$ is a monotonically increasing function of the energy consumption $\mathcal{E}$ where $\mathcal{E} = nf$. Thus given the required probability of detection, P_D, the required energy consumption $\mathcal{E}$ is uniquely known for RP. Also, any n, f minimizes the energy consumption subject to attaining P_D if nf equals the required $\mathcal{E}$. Thus for RP the energy consumption can be minimized subject to attaining the required probability of detection by either using a large number of IDS active insiders that sample traffic at a low rate, or a small number of IDS active insiders that sample traffic at a high rate. This does not however hold for the optimum algorithm as neither bound for $P_D^{\mathrm{SOPT}}(n, f, \rho)$ can be expressed in terms of nf. Nevertheless, the upper and lower bounds for $P_D^{\mathrm{SOPT}}(n, f, \rho)$ can be used to provide lower and upper bounds of the minimum energy consumption subject to attaining the required probability of detection.

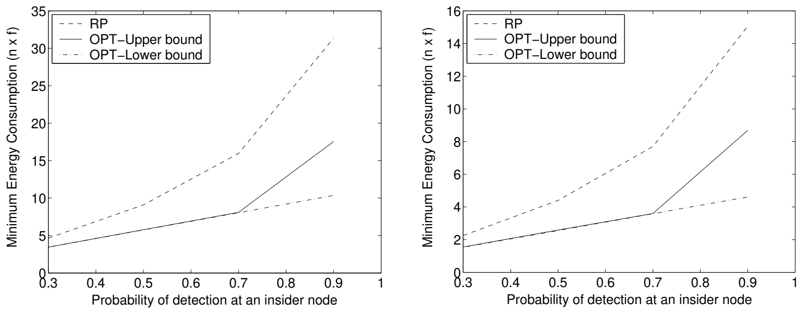
In Figures 5(a) and 5(b) we plot the minimum energy consumption (i.e., the minimum $n \times f$) and upper and lower bounds for this minimum energy consumption as functions of the required probability of detection, P_D, for RP and the optimal algorithm (OPT) respectively. We observe that the upper and lower bounds for the optimal algorithm are close except at high



(a) 100 nodes, $\rho = 0.087$

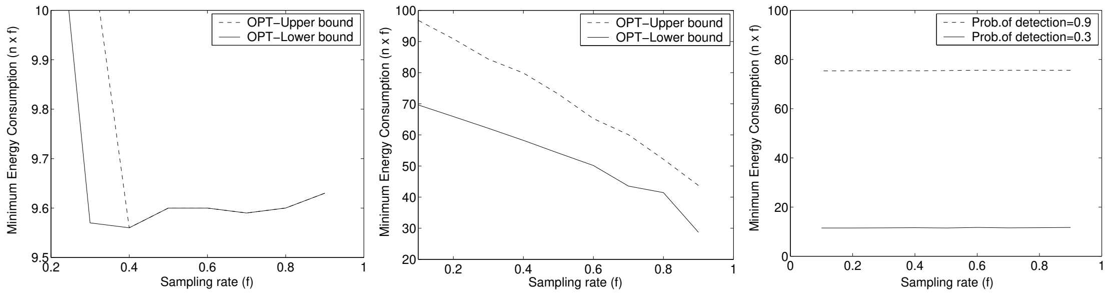
(b) 100 nodes, $\rho = 0.196$

Fig. 4. We consider topologies with 100 static insider nodes, 5 mobile intruders attacking 5 destinations. We plot the ratio of the expected number of IDS active insiders for RP and MUNEN as a function of the probability of detection of an attack.



(a) $\rho = 0.087$

(b) $\rho = 0.196$



(c) OPT, $P_D = 0.3$

(d) OPT, $P_D = 0.9$

(e) RP

Fig. 5. In figure (a) and (b), we plot the minimum energy consumption (i.e., the minimum $n \times f$) as functions of the probability of detection, P_D, for the optimal algorithm (OPT) and RP for different values of ρ. In figures (c), (d) and (e), we plot the minimum energy consumption as functions of the sampling rate for $\rho = 0.0314$ and probability of detection, P_D, $0.3, 0.9$. We consider the optimal algorithm in figures (c) and (d) and consider RP in figure (e). Here a single intruder sends a bad packet through an insider node to an outsider.

P_D, indicating that both these bounds closely approximate the minimum energy consumption in general. We also observe that both these bounds are significantly lower than RP's minimum energy consumption, and the difference progressively increases with increase in P_D. This again motivates the use of the approximately optimal MUNEN when high probability of detection is required.

The minimum value of the energy consumption decreases with increase in ρ for both the optimal algorithm and RP (Figures 5(a) and 5(b)). This is because for lower ρ each IDS active insider covers fewer insider nodes and thus either n or f need to be larger to attain the required probability of detection. Note that here we consider only the energy consumed in the detection of bad packets; the energy consumed in transmission however increases with increase in ρ.

In Figures 5(c), 5(d) and 5(e), we plot the minimum energy consumption and upper and lower bounds for this minimum energy consumption as functions of the sampling frequency f for different values of the required probability of detection, P_D, for the optimal algorithm (OPT) and RP respectively. Observe that the minimum energy consumption does not depend on f for RP. This is because, as discussed before, the energy consumption can be minimized subject to attaining the required P_D by either using a large f and small n and a small n and large f.

But, for OPT, as Figure 5(d) demonstrates, for realistic values of P_D (e.g., $P_D \geq 0.5$) the minimum energy consumption decreases with increase in f. Thus, the energy consumption is minimized when the network has few IDS active insiders (small n) that sample all packets in their neighborhood ($f = 1$). Note that the energy consumption of each insider is maximized when $f = 1$. This demonstrates that minimizing the energy consumption of the system is not equivalent to minimizing the energy consumption of individual insiders. Also, the system energy consumption is less if there exists few insiders with high energy rather than when there are several insiders with moderate energy. However, for very low P_D (e.g., $P_D = 0.3$) the energy consumption is minimized when $f = 0.4$, i.e., when the network has several IDS active insider nodes that sample packets w.p. 0.4. Thus, if the optimal algorithm is used n and f must be appropriately selected, while several different n and f can be used for RP.

We now consider some interesting generalizations. The system energy can also be minimized under the constraint that the sampling frequency f of insiders does not exceed an upper bound $f_{\max}$. Such upper bound arises when each insider needs to have a certain minimum lifetime which imposes an upper bound on its energy consumption. Next, the framework can also be generalized to consider attacks consisting of multiple (M) packets. Now, substituting $p = \alpha = 1 - f$, and $q = n/N$, Theorems 1 and 4 provide upper and lower bounds for the detection probability of the optimal algorithm ($P_D^{\text{SMOPT}}(n, f, \rho, M)$) and Theorem 3 provides the detection probability of RP ($P_D^{\text{SMRP}}(N, n, f, \rho, M)$). Finally, usually the energy consumed by an insider in receiving a packet does not depend on the distance between the transmitter and the receiver. We have therefore assumed that given n and f, $\mathcal{E}$ does not depend on ρ. If, however, the reception gain used by the insiders depend on the above distance, then $\mathcal{E} = nf\Psi(\rho)$, where Ψ is a function determined by the nature of the dependence. This case can also be considered in our framework.

VI. Conclusion

We consider ad hoc networks with unreliable insider nodes and multiple intruders. We develop a framework to counter failure of insider nodes while minimizing the resource consumption. We show that the optimal selection of the insiders that execute the detection modules is an NP-hard problem. We present a distributed polynomial complexity selection algorithm MUNEN that attains the best possible approximation ratio. We investigate a simple heuristic selection algorithm RP that ensures seamless operation in time varying topologies. Our simulations reveal that when the probability of failure is moderate to low and the security requirements are stringent, then for attaining the same level of security, the approximately optimal MUNEN consumes significantly lower resource as compared to the simple heuristic RP. Thus, MUNEN must be deployed in this case. But, when these conditions do not hold, RP attains near-optimal performance, and should be preferred. Finally, we investigate statistical detection processes and determine the optimum sampling frequencies for different selection algorithms.

We have focussed on detecting intrusions in this paper. We now describe a preliminary recovery algorithm. Here, an insider node i relaying a packet decides the packet as bad, if and only if at least one of its neighbors (which includes itself) reports it as bad. If i itself detects the packet as bad, it can drop the packet. If i does not detect the packet as bad, it relays the packet. Now, i's neighbors receive the packet in promiscuous mode only after i relays the packet. If a neighbor reports the packet as bad, i sends a report to its next hop node (which may be the destination). The report can be piggy-backed in the next data packet as well. The next hop node drops the packet if it receives such a report; it processes the packet only after waiting for a fixed time for such reports. Some optimizations are possible. First, the waiting time should be determined in accordance with the end-to-end delay requirements and transmission and processing delay at each hop. Then, if the next hop node does not receive such a report, it may mark the packet to indicate that the packet has been examined once. This avoids subsequent analysis and reduces delay and energy consumption. Recall that the IDS active insiders are selected so as to deliver the requisite detection rate even when a packet is analyzed (either correctly or incorrectly) in only one hop. Message authentication code (MAC) may be added in the reports to enhance their security. Also, MAC can be used to mark a packet that has been examined. A comprehensive investigation of the above optimizations and developing recovery schemes that are simple to implement constitutes an important topic for future research.

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.

Appendix

A. *Proof of Theorem 1*

In A.1, we state and prove a supporting lemma, Lemma 2. In A.2, we prove Theorem 1 using Lemma 2.

1) Supporting Lemma:

Lemma 2: Let $\gamma_1, \ldots, \gamma_L$ be L positive real numbers such that $\sum_{i=1}^{L} \gamma_i = 1$. Let $k_1, \ldots, k_L$ be L non-negative integers such that $k_1 < k_2 \ldots < k_L$. Then for all $r \in [0, 1]$,

$$\begin{aligned} \sum_{i=1}^{L} \gamma_i r^{k_i} \quad \geq \quad & (\lceil \sum_{i=1}^{L} \gamma_i k_i \rceil - \sum_{i=1}^{L} \gamma_i k_i) r^{\lfloor \sum_{i=1}^{L} \gamma_i k_i \rfloor} \\ & + (\sum_{i=1}^{L} \gamma_i k_i - \lfloor \sum_{i=1}^{L} \gamma_i k_i \rfloor) r^{\lceil \sum_{i=1}^{L} \gamma_i k_i \rceil}. \end{aligned}$$

Proof: Let $r \in [0, 1]$. When $\sum_{i=1}^{L} \gamma_i k_i$ is an integer, the right hand side of the inequality is 0. Hence, Lemma 2 clearly holds in this case.

Let $\sum_{i=1}^{L} \gamma_i k_i$ not be an integer. Then $z + \lambda = \sum_{i=1}^{L} \gamma_i k_i$ where $0 < \lambda < 1$ and z is an integer. Let $\mu_1 = \sum_{k_i \leq z} \gamma_i$, $\mu_2 = \sum_{k_i \geq z+1} \gamma_i$, $m_1 = \frac{\sum_{k_i \leq z} \gamma_i k_i}{\mu_1}$ and $m_2 = \frac{\sum_{k_i \geq z+1} \gamma_i k_i}{\mu_2}$.

We will prove the following relations.

$$\sum_{i=1}^{L} \gamma_i r^{k_i} \geq \mu_1 r^{m_1} + \mu_2 r^{m_2}. \tag{3}$$

$$\mu_1 r^{m_1} + \mu_2 r^{m_2} \geq \frac{m_2 - z - \lambda}{m_2 - z} r^z + \frac{\lambda}{m_2 - z} r^{m_2}. \quad (4)$$

$$\frac{m_2 - z - \lambda}{m_2 - z} r^z + \frac{\lambda}{m_2 - z} r^{m_2} \geq (1-\lambda) r^z + \lambda r^{z+1} (5)$$

The lemma follows from (3), (4) and (5) as $z = \lfloor \sum_{i=1}^{L} \gamma_i k_i \rfloor$, $z + 1 = \lceil \sum_{i=1}^{L} \gamma_i k_i \rceil$, $\lambda = \sum_{i=1}^{L} \gamma_i k_i - \lfloor \sum_{i=1}^{L} \gamma_i k_i \rfloor$ and $1 - \lambda = \lceil \sum_{i=1}^{L} \gamma_i k_i \rceil - \sum_{i=1}^{L} \gamma_i k_i$.

We now prove (3), (4) and (5). Note that $\mu_1 > 0$, $\mu_2 > 0$, $\mu_1 + \mu_2 = 1$, $m_1 \leq z$, $m_2 \geq z + 1$ and $\mu_1 m_1 + \mu_2 m_2 = z + \lambda$.

We first prove (3). Note that $\sum_i \gamma_i r^{k_i} = \sum_{k_i \leq z} \gamma_i r^{k_i} + \sum_{k_i \geq z+1} \gamma_i r^{k_i}$. Clearly, $\gamma_i / \mu_j > 0$, for each $i \in \{1, \ldots, L\}$, $j \in \{1, 2\}$. Also, $\frac{\sum_{k_i \leq z} \gamma_i}{\mu_1} = 1$ and $\frac{\sum_{k_i \geq z+1} \gamma_i}{\mu_2} = 1$. Thus, from convexity of $f(k) = r^k$, we have $\sum_{k_i \leq z} \frac{\gamma_i}{\mu_1} r^{k_i} \geq r^{m_1}$ and $\sum_{k_i \geq z+1} \frac{\gamma_i}{\mu_2} r^{k_i} \geq r^{m_2}$. Thus, $\sum_{k_i \leq z} \gamma_i r^{k_i} \geq \mu_1 r^{m_1}$ and $\sum_{k_i \geq z+1} \gamma_i r^{k_i} \geq \mu_2 r^{m_2}$. Thus, (3) follows.

We next prove (4). It suffices to prove that $\mu_1 r^{m_1} + \frac{\mu_2 m_2 - \mu_2 z - \lambda}{m_2 - z} r^{m_2} \geq \frac{m_2 - z - \lambda}{m_2 - z} r^z$. Now, since $\mu_1 m_1 + \mu_2 m_2 = z + \lambda$, and $\mu_1 + \mu_2 = 1$, $\mu_2 m_2 - \mu_2 z - \lambda = \mu_1 (z - m_1)$. Thus,

$$\begin{aligned}
& \mu_1 r^{m_1} + \frac{\mu_2 m_2 - \mu_2 z - \lambda}{m_2 - z} r^{m_2} \\
= \; & \mu_1 r^{m_1} + \mu_1 \frac{z - m_1}{m_2 - z} r^{m_2} \\
= \; & \mu_1 \frac{m_2 - m_1}{m_2 - z} \left[\frac{(m_2 - z) r^{m_1} + (z - m_1) r^{m_2}}{m_2 - m_1} \right] \\
\geq \; & \mu_1 \frac{m_2 - m_1}{m_2 - z} r^z \\
= \; & \frac{m_2 - z - \lambda}{m_2 - z} r^z \\
& \text{(since } \mu_1 m_1 + \mu_2 m_2 = z + \lambda \text{ and } \mu_1 + \mu_2 = 1).
\end{aligned}$$

The inequality follows from the convexity of $f(k) = r^k$, and since $m_2 - m_1 \geq m_2 - z > 0$. Thus, (4) holds.

Finally, we prove (5). Now,

$$\begin{aligned}
& \frac{m_2 - z - \lambda}{m_2 - z} r^z + \frac{\lambda}{m_2 - z} r^{m_2} - (1 - \lambda) r^z \\
= \; & \lambda \left((1 - \frac{1}{m_2 - z}) r^z + \frac{1}{m_2 - z} r^{m_2} \right) \\
\geq \; & \lambda r^{z+1} \text{ (since } f(k) = r^k \text{ is convex and } m_2 \geq z + 1).
\end{aligned}$$

Thus, (5) holds. ■

2) Proof of Theorem 1:

Proof: Let the optimal algorithm select the IDS active insiders such that γ_i fraction of the total area is covered by k_i IDS active insiders, where $\sum_{i=1}^{L} \gamma_i = 1$, $\gamma_i > 0$ for all $i = 1, \ldots L$ and $L \leq n + 1$ and $0 \leq k_1 < k_2 < .. < k_L \leq n$. Since there are n IDS active insiders, and each covers ρ fraction of the total area, $\sum_{i=1}^{L} \gamma_i k_i = n\rho$. Since the insider v that relays the bad packets is uniformly selected and all points in the square are insider nodes, v is uniformly distributed in the square. Thus, $P_D^{\text{OPT}}(n, p, \rho, M) = 1 - \sum_{i=1}^{L} \gamma_i r^{k_i}$, where $r = 1 - (1-p)(1-\alpha)^{M-1}$. First let $n\rho$ be an integer. The result follows from the convexity of the function $f(k) = r^k$ for any $k \geq 0$ and since $\sum_{i=1}^{L} \gamma_i k_i = n\rho$. When $n\rho$ is not an integer, the result follows from Lemma 2 and since $\sum_{i=1}^{L} \gamma_i k_i = n\rho$. ■

B. Proof of Theorem 2

We first outline the proof. We consider a hybrid algorithm $\mathcal{A}_i$ that selects insiders as per Greedy in the first i iterations and then selects insiders as per MUNEN in the remaining iterations. Clearly, Greedy and MUNEN are $\mathcal{A}_N$ and $\mathcal{A}_0$ respectively. We prove that for each i, $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ select the same set of insiders. Thus, MUNEN and Greedy select the same set of insiders.

This subsection is organized as follows. In B.1, we first define the terminologies which we use throughout the proof. In B.2, we state and prove a lemma that we use to prove Theorem 2. In B.3, we prove Theorem 2.

1) Terminologies:

Definition 2: Let $A \subseteq V'$. An insider u is *satisfied under A* if it is covered by at least k insiders in A, and *unsatisfied under A* otherwise.

If A is the set of IDS active insiders, the $k-$priority of an insider u is the number of neighbors of u that are unsatisfied under A, and is denoted as $US_A(u)$.

Definition 3: Let $A \subseteq V'$. An insider u is *globally optimum* under A if (a) $u \in V' \setminus A$ (b) $US_A(u) > 0$ and (c) u has the maximum $US_A(u)$ in $V' \setminus A$. If multiple insiders satisfy the above criteria, the one that has the minimum identity amongst them is considered to be globally optimum.

Definition 4: Let $A \subseteq V'$. An insider u is *extended neighborhood optimum* under A if (a) $u \in V' \setminus A$ (b) $US_A(u) > 0$ and (c) for every $v \in N^2(u) \setminus A$ (i) either $US_A(u) > US_A(v)$ (ii) or $US_A(u) = US_A(v)$ and $u < v$. LOCAL(A) is the set of the extended neighborhood optimum insiders under A.

Thus, by definition, no two insiders in LOCAL(A) can be within two hops of each other.

Let G_0 be the set of insiders selected by $\mathcal{A}_i$ at the end of iteration i. Let $G_0 \cup D_0$ be the set of insiders selected by $\mathcal{A}_{i+1}$ at the end of iteration $i + 1$. If $\mathcal{A}_{i+1}$ terminates at the end of iteration $1, \ldots, i$, then $D_0 = \phi$, otherwise $|D_0| = 1$. In the latter case, let $D_0 = \{v_{i+1}\}$.

Let j^{MUNEN} denote the j^{th} iteration of executing MUNEN. Let X_j be the set of insiders selected by $\mathcal{A}_i$ just before iteration j^{MUNEN} and W_j be the set of insiders selected by $\mathcal{A}_{i+1}$ just before iteration j^{MUNEN} where $j = 1, 2, \ldots$. Clearly, $X_1 = G_0$ and $W_1 = G_0 \cup D_0$. Let $W_0 = W_1 \setminus D_0 = G_0$.

Let Y_j be the set of insiders selected in iteration j^{MUNEN} of $\mathcal{A}_i$ and Z_j be the set of insiders selected in iteration j^{MUNEN} of $\mathcal{A}_{i+1}$ where $j = 1, 2, \ldots$. By definition, $Y_j = \text{LOCAL}(X_j)$ and $Z_j = \text{LOCAL}(W_j)$.

If $U \subseteq V, W \subseteq V$, and $U \neq \phi, V \neq \phi$, the minimum distance $d(U, W)$ between the insiders in U and W is $\min_{u \in U, v \in W} h(u, v)$.

2) Supporting Lemma:

Lemma 3: Let $\mathcal{A}_{i+1}$ not terminate at the end of iteration i. There exist sets $D_1, D_2, \ldots$ and $S_0, S_1, \ldots$ such that for all $m = 0, 1, ...$

1) $US_{X_{m+1}}(u) = US_{W_m}(u), \forall\, u \in D_m$,
2) $W_{m+1} = X_{m+1} \cup D_m$,
3) $D_m \cap S_m = \phi, Y_{m+1} = D_m \cup S_m$,
4) $US_{X_{m+1}}(u) = US_{W_{m+1}}(u), \forall\, u \in S_m$,
5) $X_{m+2} = W_{m+1} \cup S_m$ and
6) $D_{m+1} \cap S_m = \phi, Z_{m+1} = S_m \cup D_{m+1}$.

Proof: Since $\mathcal{A}_{i+1}$ does not terminate at the end of iteration i, $D_0 = \{v_{i+1}\}$. We prove the lemma using induction.

We first consider $m = 0$.

Since $G_0 = X_1 = W_0$, $US_{X_1}(u) = US_{W_0}(u)\ \forall\ u \in D_0$. Thus, (1) follows.

Now, $W_1 = G_0 \cup D_0 = X_1 \cup D_0$. Thus, (2) follows.

We now prove that there exists a set S_0 such that (3), (4) and (5) hold.

Note that $Y_1 = \text{LOCAL}(X_1)$. Let us consider the 1^{MUNEN} iteration or the $(i+1)^{th}$ iteration of $\mathcal{A}_i$. Note that $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ select the same insiders in the same order in the first i iterations. Therefore, in these iterations, when an insider v is selected by $\mathcal{A}_i$, it has the same number of unsatisfied neighbors as when it is selected by $\mathcal{A}_{i+1}$. Since the insider v_{i+1} is selected by Greedy at the $(i+1)^{th}$ iteration of $\mathcal{A}_{i+1}$, v_{i+1} is globally optimum under G_0 and hence it is also extended neighborhood optimum under G_0. Since $X_1 = G_0$, $v_{i+1} \in \text{LOCAL}(X_1)$, and hence $D_0 \subseteq \text{LOCAL}(X_1) = Y_1$. Let $S_0 = Y_1 \setminus D_0$. Clearly, (3) holds.

From (3), $D_0 \cup S_0 = Y_1 = \text{LOCAL}(X_1)$ and $D_0 \cap S_0 = \phi$. Thus, if $S_0 \neq \phi$, $d(D_0, S_0) \geq 3$. Thus,

a) $US_{X_1}(u) = US_{X_1 \cup D_0}(u), \forall\ u \in S_0$, and
b) $US_{X_1}(u) \geq US_{X_1 \cup D_0}(u), \forall\ u$.

Now, (4) follows from (2) and (a).

Now, $X_2 = X_1 \cup Y_1$. Now, from (3) and since $X_1 = G_0$, $X_2 = G_0 \cup D_0 \cup S_0$. Since $W_1 = G_0 \cup D_0$, $X_2 = W_1 \cup S_0$. Thus, (5) holds.

We now show that there exists a set D_1 such that (6) holds. Since $D_0 \cup S_0 = \text{LOCAL}(X_1)$, each insider in S_0 is extended neighborhood optimum under X_1. Thus, $S_0 \subseteq V' \setminus X_1$. Hence, from (3), $S_0 \subseteq V' \setminus (X_1 \cup D_0)$. Now, from (a) and (b), it follows that each insider in S_0 is also extended neighborhood optimum under $X_1 \cup D_0$. Hence, $S_0 \subseteq \text{LOCAL}(X_1 \cup D_0) = \text{LOCAL}(W_1) = Z_1$. Let $D_1 = Z_1 \setminus S_0$. Clearly, (6) holds. Thus, the base case holds.

We now assume that there exists sets $D_1, D_2, \ldots, D_l$ and $S_0, S_1, \ldots S_{l-1}$ such that (1) to (6) hold for $m = 0, 1, \ldots, l-1$. We prove that there exists sets D_{l+1}, S_l such that (1) to (6) hold for $m = l$.

From (6) of induction hypothesis, $S_{l-1} \cup D_l = Z_l = \text{LOCAL}(W_l)$, and $D_l \cap S_{l-1} = \phi$. Thus, if $S_{l-1} \neq \phi$ and $D_l \neq \phi$, $d(S_{l-1}, D_l) \geq 3$. Hence, $US_{W_l \cup S_{l-1}}(u) = US_{W_l}(u)$ for each $u \in D_l$. From (5) of induction hypothesis, $W_l \cup S_{l-1} = X_{l+1}$. Now, (1) follows from the above.

Now, $W_{l+1} = W_l \cup Z_l$. Now, from (6) of induction hypothesis, $W_{l+1} = W_l \cup S_{l-1} \cup D_l$. Next, from (5) of induction hypothesis, $W_{l+1} = X_{l+1} \cup D_l$. Thus, (2) holds.

We now show that there exists a set S_l such that (3), (4) and (5) hold.

Since from (6) of induction hypothesis, $S_{l-1} \cup D_l = Z_l = \text{LOCAL}(W_l)$, each insider in D_l is extended neighborhood optimum under W_l. Thus, $D_l \subseteq V' \setminus W_l$. Now, since from (6) of induction hypothesis, $D_l \cap S_{l-1} = \phi$, $D_l \subseteq V' \setminus (W_l \cup S_{l-1})$. Now, from (5) of induction hypothesis, $D_l \subseteq V' \setminus X_{l+1}$. Again, since from (5) of induction hypothesis, $W_l \subseteq X_{l+1}$, $US_{X_{l+1}}(u) \leq US_{W_l}(u)\ \forall\ u$. Now, from (1), each insider in D_l is extended neighborhood optimum under X_{l+1}. Thus, $D_l \subseteq \text{LOCAL}(X_{l+1}) = Y_{l+1}$. Let $S_l = Y_{l+1} \setminus D_l$. Clearly, S_l satisfies (3).

From (3), $D_l \cup S_l = Y_{l+1} = \text{LOCAL}(X_{l+1})$, and $D_l \cap S_l = \phi$. Thus, if $D_l \neq \phi$, $S_l \neq \phi$, $d(D_l, S_l) \geq 3$. Hence,

i) $US_{X_{l+1}}(u) = US_{X_{l+1} \cup D_l}(u), \forall\ u \in S_l$, and
ii) $US_{X_{l+1}}(u) \geq US_{X_{l+1} \cup D_l}(u), \forall\ u$.

Now, (4) follows from (2) and (i).

Now, $X_{l+2} = X_{l+1} \cup Y_{l+1}$. Thus, from (3), $X_{l+2} = X_{l+1} \cup D_l \cup S_l$. Next, from (2), $X_{l+2} = W_{l+1} \cup S_l$. Thus, (5) holds.

We now show that there exists a set D_{l+1} such that (6) holds. From (3) $D_l \cup S_l = Y_{l+1} = \text{LOCAL}(X_{l+1})$. Thus, each insider in S_l is extended neighborhood optimum under X_{l+1}. Thus, $S_l \subseteq V' \setminus X_{l+1}$. Now, since from (3), $D_l \cap S_l = \phi$, $S_l \subseteq V' \setminus (X_{l+1} \cup D_l)$. Now, from (i) and (ii), it follows that each insider in S_l is also extended neighborhood optimum under $X_{l+1} \cup D_l$. Hence, $S_l \subseteq \text{LOCAL}(X_{l+1} \cup D_l) = \text{LOCAL}(W_{l+1}) = Z_{l+1}$. Let $D_{l+1} = Z_{l+1} \setminus S_l$. Clearly, D_{l+1} satisfies (6).

Thus, (1) to (6) hold for all m. ■

3) Proof of Theorem 2:

Proof: We first prove that $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ select the same set of insiders. Let $\mathcal{A}_{i+1}$ terminate just before iteration j^{MUNEN}, where $j \geq 1$. Thus, $Z_j = \phi$. Thus, $W_j = W_{j+1}$. Also, from (6) of lemma 3, $S_{j-1} = D_j = \phi$. Thus, from (3) of lemma 3, $Y_j = D_{j-1}$. From (2) of lemma 3, $W_{j+1} = X_{j+1}$. Also, $Z_{j+1} = \phi$. Thus, as before, $S_j = \phi$. Thus, $Y_{j+1} = D_j \cup S_j = \phi$. Thus, $\mathcal{A}_i$ terminates at the end of iteration j^{MUNEN}. The result follows since $X_{j+1} = W_{j+1} = W_j$.

Let $\mathcal{A}_{i+1}$ terminate at the end of j iterations, $j \leq i$. The result follows since $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ select insiders in the same manner before the end of i iterations.

Hence, $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ select the same set of insiders. Thus, $\mathcal{A}_0$ (MUNEN) and $\mathcal{A}_N$ (Greedy) select the same set of insiders. ■

C. Proof of Theorem 3

Proof of Theorem 3: Let insider node V relay the bad packets. Now, the attack is not detected if V does not detect all packets (event X) and no other insider node covered by V detects all packets (event Y). These events are independent. The complement of event X happens if and only if V is IDS active and V is OI during the transmission of each packet. Both these are independent events. Under RP, V is IDS active w.p. q. Also, V is OI during the transmission of each packet w.p. $(1-p)(1-\alpha)^{M-1}$. Thus event X happens w.p. $1 - q(1-p)(1-\alpha)^{M-1}$. Thus, $P_D^{\text{RP}}(N, q, p, \rho, M) = 1 - \left(1 - q(1-p)(1-\alpha)^{M-1}\right) \Pr(Y)$. Like V, an insider node covered by V detects all bad packets w.p. $q(1-p)(1-\alpha)^{M-1}$. Thus, $\Pr(Y)$ is given by Pr (Q) in Lemma 3 in appendix of [6] with $t = q(1-p)(1-\alpha)^{M-1}$. The result follows.

D. Statement and Proof of Theorem 4

Theorem 4: Consider the ETICDS(ρ) model. Let $\sqrt{\pi/\rho}$ be an even integer. Let $n_1 = \frac{\pi}{4\rho}, n_2 = \frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} + 1, n_3 = \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} - 3, n_4 = \frac{\pi}{2\rho} + \sqrt{\frac{\pi}{\rho}} + 1, r = 1 - (1-p)(1-\alpha)^{M-1}$

$$P_D^{\text{OPT}}(n, p, \rho, M) \geq$$

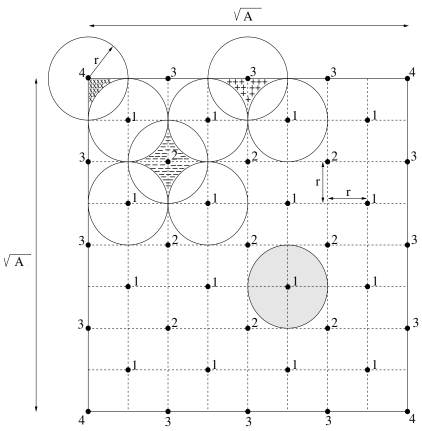


Fig. 6. The figure illustrates an algorithm for selecting IDS in an area where every point is an insider node. The algorithm would execute IDS in insider nodes at the positions marked 1, 2, 3, 4. The circles indicate the coverage areas of the insider nodes that are currently executing the IDS.

$$
\begin{cases}
n\rho(1-r), \text{ if } n \le n_1 \\
\frac{\pi}{4}(1-r) + \rho(n - \frac{\pi}{4\rho})\left(\frac{4(1-r)^2}{\pi} - (1-2r)(1-r)\right), \\
\text{ if } n_1 < n \le n_2 \\
\frac{\pi}{4}(1-r) + \rho(n - \sqrt{\frac{\pi}{\rho}} + 1)\left(\frac{2(1-r)^2}{\pi} - \frac{(1-2r)(1-r)}{2}\right), \\
\text{ if } n_2 < n \le n_3 \\
\frac{\pi}{4}(1-r) + \rho(n + \frac{\pi}{2\rho} - \sqrt{\frac{\pi}{\rho}} - 1)\left(\frac{(1-r)^2}{\pi} - \frac{(1-2r)(1-r)}{4}\right), \\
\text{ if } n_3 < n \le n_4 \\
1 - (2-r)r + \frac{\pi}{2}(1-r)r + \rho(n-n_4)\times \\
\left(\frac{4r(1-r)^2}{\pi} - r(1-2r)(1-r)\right), \text{ if } n_4 < n \le n_4 + n_1 \\
1 - \frac{(4-\pi)}{4}r(1+r) + \frac{(2-\pi)}{2}r^3 + (n - n_4 + n_1)\times \\
\left(\frac{4r(1-r)(1-r^2)}{\pi} - r(1-r)(1-2r^2)\right), \\
\text{ if } n_4 + n_1 < n \le n_4 + n_2 \\
1 - \frac{4-\pi}{4}r(2+r) - \frac{(4-\pi)}{\pi}r\rho\left((1-r)(\sqrt{\frac{\pi}{\rho}} - 1)\right. \\
\left. - \frac{\pi}{4\rho}(2-r)\right) + 2\rho\frac{(2-\pi)}{\pi}r^3\left((1-r)(\sqrt{\frac{\pi}{\rho}} - 1) + \frac{r\pi}{4\rho}\right) \\
+(n - n_4 + n_2)r\rho\left(\frac{(1-r)}{2\pi}\left(4(1-r^2) - \pi(1-2r^2)\right)\right), \\
\text{ if } n_4 + n_2 < n \le n_4 + n_3 \\
1 - \frac{(4-\pi)}{4}\left(2r^2 + \frac{4r\rho}{\pi}(1-r)\right) + \rho\frac{(2-\pi)}{\pi}r^3\left(2(1-r) + \frac{r\pi}{2\rho}\right) \\
+(n - n_4 + n_3)\frac{\rho r(1-r)}{4\pi}\left(4(1-r^2) - \pi(1-2r^2)\right), \\
\text{ if } n_4 + n_3 < n \le 2n_4 \\
1 - \frac{(4-\pi)}{2}r^k(1 - r^{k-1}) - r^{2k} + (n - kn_4)\rho(1-r)r^k\times \\
\left(\frac{4(1-r^k)}{\pi} - (1-2r^k)\right), \text{ if } kn_4 < n \le kn_4 + n_1, \ k \ge 2 \\
1 - \frac{(4-\pi)}{4}r^k(1 + r - r^{k+1}) - \frac{\pi}{4}r^{2k+1} \\
+(n - (kn_4 + n_1))\rho(1-r)r^k\left(\frac{4(1-r^{k+1})}{\pi} - (1-2r^{k+1})\right), \\
\text{ if } kn_4 + n_1 < n \le kn_4 + n_2 \\
1 - r^k\left((4-\pi)(\frac{1}{2} - \frac{n_2\rho(1-r)}{\pi})\right) \\
+2\rho\frac{(2-\pi)}{\pi}r^{2k+1}\left((1-r)(\sqrt{\frac{\pi}{\rho}} - 1) + \frac{r\pi}{4\rho}\right) \\
+(n - (kn_4 + n_2))\rho(1-r)r^k\left(\frac{2(1-r^{k+1})}{\pi} - \frac{(1-2r^{k+1})}{2}\right), \\
\text{ if } kn_4 + n_2 < n \le kn_4 + n_3 \\
1 - \frac{(4-\pi)r^k\rho}{\pi}\left((1-r) + \frac{r\pi}{2\rho}\right) + \rho\frac{(2-\pi)}{\pi}r^{2k+1}\times \\
\left(2(1-p) + \frac{r\pi}{2\rho}\right) + (n - (kn_4 + n_3))r^k\rho(1-r)\times \\
\left(\frac{(1-r^{k+1})}{\pi} - \frac{(1-2r^{k+1})}{4}\right), \text{ if } kn_4 + n_3 < n \le (k+1)n_4.
\end{cases}
$$

Proof: We propose a specific algorithm (OPTLB) for selecting n IDS active insiders, when all points in the square are insiders. Let OPTLB attain a probability of detection $P_D^{\text{OPTLB}}(n,p,\rho,M)$. Clearly, $P_D^{\text{OPT}}(n,p,\rho,M) \ge P_D^{\text{OPTLB}}(n,p,\rho,M)$.

We now describe OPTLB using Figure 6. Insider nodes are first selected at positions marked '1', next at positions marked '2', next at positions marked '3,' next at positions marked '4,' again at positions marked '1' and so on. OPTLB terminates when n insider nodes are selected.

Given n, OPTLB selects the IDS active insiders such that $\gamma_i(n)$ fraction of the total area is covered by $k_i(n)$ IDS active insiders, where $\sum_j \gamma_j = 1$ and $0 \le k_1(n) < k_2(n) < ...$ Since the insider V that relays the bad packets is uniformly selected and all points in the square are insiders, V is uniformly distributed in the square. Thus, $P_D^{\text{OPTLB}}(n,p,\rho,M) = 1 - \sum_j \gamma_j(n) r^{k_j(n)}$, where $r = 1-(1-p)(1-\alpha)^{M-1}$.

When all positions marked '1, 2, 3, 4' consist of k IDS active insiders each, then $k_1(n) = k$. There are n_i positions marked 'i', for $i \in \{1,2,3,4\}$. Now, $\gamma_j(n)$ and $k_j(n)$ can be computed for each j, n after some algebra [5]. Thereby, $P_D^{\text{OPTLB}}(n,p,\rho,M)$ can be computed [5]. This provides the lower bound. The result follows. ■

Refer to technical report [5] for the lower bound for $P_D^{\text{OPT}}(n,p,\rho,M)$ when $\sqrt{\pi/\rho}$ is not an even integer.

E. Proof for Theorem 1 of [6]

We prove Theorem 1 of [6] using the results we obtained for MUNEN in Subsection B. In E.1, we first define some terminologies. Then, in E.2, we state and prove supporting lemmas 4 and 5. Finally, in E.3, we prove Theorem 1 of [6].

1) Terminologies:

Definition 5: Let $A \subseteq V'$. The span of insider $v \in V$, $\text{span}_A(v)$, is the tuple $(US_A(v), v)$.

We define an ordering on the spans. Let $\text{span}_A(v) = (v_1, v_2)$ and $\text{span}_W(u) = (u_1, u_2)$. Now, $\text{span}_A(v) < \text{span}_W(u)$ if (i) $v_1 < u_1$ or (ii) $v_1 = u_1$ and $v_2 > u_2$.

Clearly, if $u \ne v$, for any A, $\text{span}_A(v) \ne \text{span}_A(u)$.

Let $MD(j)$ ($GD(j)$) be the set of insiders selected by MUNEN (Greedy) just before the j^{th} iteration. Thus, $MD(|V'|+1)$ ($GD(|V'|+1)$) is the set of insiders selected by MUNEN (Greedy) after its termination. From Theorem 2, $MD(|V'|+1) = GD(|V'|+1)$. We denote these sets by I. Let T_j be the set of insiders selected in the j^{th} iteration of MUNEN i.e., $T_j = MD(j+1) \setminus MD(j)$.

Definition 6: Let $v \in I$. The *span-select-MUNEN* of v is $\text{span}_{MD(j)}(v)$ if MUNEN selects v in the j^{th} iteration. The *span-select-Greedy* of v is $\text{span}_{GD(j)}(v)$ if Greedy selects v in the j^{th} iteration.

2) Supporting Lemmas:

Lemma 4: If $v \in I$, its *span-select-MUNEN* and *span-select-Greedy* are identical.

Proof: Let $v \in I$. From Theorem 2, for any $i, j \in \{0,\ldots,N\}$, both $\mathcal{A}_i$ and $\mathcal{A}_j$ select v. Let P_i be the set of insiders $\mathcal{A}_i$ selects just before $\mathcal{A}_i$ selects v. We will prove that $US_{P_i}(v) = US_{P_j}(v)$. Thus, $US_{P_0}(v) = US_{P_N}(v)$. The lemma now follows.

We now prove that $US_{P_i}(v) = US_{P_j}(v)$ for any $v \in I$ and $i, j \in \{0, \ldots, N\}$. Clearly, it is sufficient to prove the result for i, j such that $i < N$ and $j = i + 1$. Let $\mathcal{A}_i$ select v in iteration l. Let $l \leq i$. Since $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ select the same insiders in each iteration $1, \ldots, i$, the result holds. Now, let $l > i$, i.e., $v \in Y_m$ for some m, where $m \geq 1$. Then $P_i = X_m$. From (3) of lemma 3, $v \in D_{m-1}$ or $v \in S_{m-1}$. Let $v \in S_{m-1}$. From (6) of lemma 3, $v \in Z_m$. Then $P_{i+1} = W_m$. The result follows from (4) of lemma 3. Now, let $v \in D_{m-1}$. Let $m > 1$. From (6) of lemma 3, $v \in Z_{m-1}$. Then $P_{i+1} = W_{m-1}$. The result follows from (1) of lemma 3. Now, let $m = 1$, i.e., $v \in D_0$. Thus, $\mathcal{A}_{i+1}$ selects v in iteration $i+1$. Thus, $P_{i+1} = G_0 = W_0$. The result follows from (1) of lemma 3. ■

Since $MD(j) \subseteq MD(j+1)$, for any $u \in V$, $US_{MD(j)}(u) \geq US_{MD(j+1)}(u)$. Thus,

$$\text{span}_{MD(j)}(u) \geq \text{span}_{MD(j+1)}(u),\ \forall\, u \in V. \qquad (6)$$

Lemma 5: For any iteration j of MUNEN, $\exists\ v \in T_j$ such that $\text{span}_{MD(j)}(v) > \text{span}_{MD(j+1)}(u)\ \forall\, u \in T_{j+1}$.

Proof: Let there not exist $v \in T_j$ such that $\text{span}_{MD(j)}(v) > \text{span}_{MD(j+1)}(u)\ \forall\ u \in T_{j+1}$. Now, for all $v \in T_j$ and $u \in T_{j+1}$, since $v \neq u$ if $v \in T_j$ and $u \in T_{j+1}$, $\text{span}_{MD(j)}(v) \neq \text{span}_{MD(j+1)}(u)$. Therefore, for each $v \in T_j$, there must exist some $u \in T_{j+1}$ such that $\text{span}_{MD(j+1)}(u) > \text{span}_{MD(j)}(v)$. Thus, there must exist at least one $u_0 \in T_{j+1}$ such that $\text{span}_{MD(j+1)}(u_0) > \text{span}_{MD(j)}(v)\ \forall\ v \in T_j$. From (6), $\text{span}_{MD(j)}(u_0) \geq \text{span}_{MD(j+1)}(u_0)$. Thus, $\text{span}_{MD(j)}(u_0) > \text{span}_{MD(j)}(v)\ \forall\, v \in T_j$.

Since $u_0 \in T_{j+1}$, $u_0 \in V' \setminus MD(j)$, $US_{MD(j)}(u_0) \geq US_{MD(j+1)}(u_0) > 0$, and MUNEN does not select u_0 in the j^{th} iteration. Thus, there exists an insider $u_1 \in N^2(u_0) \setminus MD(j)$ such that $\text{span}_{MD(j)}(u_0) < \text{span}_{MD(j)}(u_1)$. Again, either MUNEN selects u_1 in the j^{th} iteration, or there exists an insider $u_2 \in N^2(u_1) \setminus MD(j)$ such that $\text{span}_{MD(j)}(u_1) < \text{span}_{MD(j)}(u_2)$. Since the number of insiders is finite, continuing in this manner, we obtain an insider u_p such that $\text{span}_{MD(j)}(u_0) < \text{span}_{MD(j)}(u_p)$ and $u_p \in T_j$. But, this contradicts the fact that $\text{span}_{MD(j)}(u_0) > \text{span}_{MD(j)}(v)\ \forall\, v \in T_j$. ■

3) Proof for Theorem 1 of [6]:

Proof: Let $k = 1$. Note that Greedy-MC and Greedy select the same set of insiders in each of the first n iterations. The only difference between the two is that, unlike Greedy, Greedy-MC must terminate after at most n iterations. Thus, the set of insiders selected by Greedy-MC is $GD(n + 1)$. Also, in its node-selection phase, in every iteration MUNEN-MC selects the same set of insiders as MUNEN. The node-selection phase continues for n iterations. During the subsequent node-retention phase, MUNEN-MC retains those insiders in $MD(n + 1)$ that have n highest *span-select-MUNEN* in $MD(n + 1)$. We therefore need to prove that when $k = 1$, insiders in $GD(n + 1)$ constitute the insiders with n highest *span-select-MUNEN* in $MD(n + 1)$. We next prove this for any k.

The insiders in $GD(n + 1)$ constitute the insiders with n highest *span-select-Greedy* in I. Hence, from lemma 4, the insiders in $GD(n + 1)$ constitute the insiders with n highest *span-select-MUNEN* in I. It is now sufficient to prove that the insiders with n highest *span-select-MUNEN* in $MD(n+1)$ are those with n highest *span-select-MUNEN* in I. Since $n \leq N$, $MD(n + 1) \subseteq MD(N + 1) = I$. Now, from lemma 5, we know that there exists at least n insiders in $MD(n + 1)$ that have higher *span-select-MUNEN* than $u\ \forall\, u \in I \setminus MD(n+1)$. The result follows. ■

References

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

[2] M. R. Garey and D. S. Johnson. *Computers and Intractability*. W. H. Freeman and Company, 2000.

[3] C. Poellabauer and K. Schwan. Energy-aware traffic shaping for wireless real-time applications. In *Proceedings of the 10th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pages 48–55, May 2004.

[4] T. Ptacek and T. Newsham. Insertion, evasion, and denial of service: Eluding network intrusion detection. Technical report, an SNI Technical Report, http://www.aciri.org/vern/Ptacek-Newsham-Evasion-98.ps, Jan. 1998.

[5] D. Subhadrabandhu, S. Sarkar, and F. Anjum. Misuse detection with compromised defenders in adhoc networks. Technical report, University of Pennsylvania Technical Report, http://www.seas.upenn.edu/∼swati/publication.htm, July 2004.

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

[7] V. Vazirani. *Approximation Algorithms*. Springer, 2001.

[8] 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.

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 the Fu foundation School of Engineering and Applied Science, Columbia University, New York, in 1997. From 1997 to 2000, he was involved in designing international transmission systems and network planning at the Communications Authority of Thailand (CAT) and participated in corporatization of CAT. 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 Master of Engineering in Electrical Communication Engineering from the Indian Institute of Science in 1996 and 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 the Motorola gold medal for the best masters student in the division of Electrical Sciences at the Indian Institute of Science and 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.