A Study on Proposed Distributed Attack Detection Algorithm Using Experimental and Simulation Analysis

Siva Balaji Yadav.C[1], R.Seshadri,PhD[2]
[1]*(Computer Science and Engineering, SV University, Tirupati, India)*
[2]*(SVU Computer center, SV University, Tirupati, India)*

Abstract: *The attack detection rates are higher for large node deployment densities, as compared to the low density counterparts. This is because the attack detection scheme relies on both the individual traffic observations by the detector nodes, as well as the subsequent verification and reconstruction of observed traffic sub patterns by the detector nodes as well as the mGN nodes, for classification purposes. In this work, we evaluated the performance of our proposed distributed attack detection scheme, through experiments and simulation analysis. The scheme proposed, performs distributed denial of service attack detection, in the presence of injected nodes, inclusive of laptop-class nodes, in the network. As part of the detection process, detector nodes monitor network traffic flow towards a set of victim nodes, and further, reconstruct patterns of observed network traffic, to facilitate attack decision making. The performance of the scheme is affected by several algorithmic as well as network parameters, which need to be defined, at network initialization time. We studied the effect of variation of these algorithmic and network-level parameters on the outcomes of the proposed attack detection scheme. We quantified the results obtained for variations in these parameter values, based on simulation experiments. The metrics that are compared and analyzed as part of the simulation experiment are: attack detection rate, false positive rate, false negative rate and detector/mGN node energy utilization rates. We also performed a comparative analysis of the acquired experimental results for the proposed scheme, with corresponding results obtained from the simulation of a centralized Self Organizing Map-based attack detection scheme. The purpose of this comparison is to establish the superiority of the proposed distributed pattern recognition approach over other centralized techniques for detection of distributed denial of service attacks in wireless sensor networks.*

Keywords: *Algorithm, distributed denial of service attacks, wireless sensor networks, Map-based attack detection scheme*

I. Introduction

The intensity of the attack traffic increases with corresponding increase in the total number of adversarial nodes in the network, assuming participation of all such nodes in the attack process (1-3). If the adversarial nodes are placed at multiple locations in the network, the traffic intensity will increase from several ends of the network, thus comprising a distributed denial of service attack (4, 5). The algorithmic parameters associated with the attack detection algorithm are: optimal time epoch length (Δ_{opt}), number of detector GN nodes *n*, and the pattern update rates for each of the *r* target nodes. The network-level parameters that affect the outcomes of the detection scheme are: node deployment densities and initial node energy contents (6-8). The overall effect of the attack detection through a SOM-based centralized mechanism is compared with results acquired for our proposed scheme, under variations of the parameter values (9). Higher detection rates imply quicker response times by the base station in replacement or reallocation of the victim node tasks to other nodes. Lower detection rates imply rapid exhaustion of the energy contents within the target nodes, thus reducing the overall functionality of the network. The false alarm rates of the scheme are also studied to analyse the short-comings of the algorithm, under variations in the parameter values (10). False positive rates imply the incorrect classification of legitimate network packets as attack packets by the detection scheme. Higher values of false positive rates will lead to the incorrect reallocation and/or replacement of sensor nodes, assumed to be under an attack (11). False negative rates are defined as the rate at which the detection scheme classifies malicious packets as legitimate packets. Higher false negative rates imply that the detection rate has faltered in its task of accurately detecting attacks, and therefore will lead to higher success, in terms of rapid energy exhaustion of the victim nodes, by the attacker nodes. The energy decay rate of the individual sensor nodes provides an estimate on the expected lifetimes of the nodes. Higher energy decay rates will lead to rapid decline in the network resources, and reduce the overall life- time of the network. Considering the inaccessibility of most sensor networks post-deployment, it is very crucial to safeguard the limited on-node energy resources. We therefore analysed the effect of the detection process on the energy content of the GN as well as the mGN nodes of the network, to derive results justifying an ideal ratio of these nodes, to facilitate scheme operation with minimal energy overhead, without compromising the accuracy in attack detection (12).

DOI: 10.9790/0661-1803060110

II. Methodology

The Our initial experiments are performed to study the attack detection rates for variations in the network traffic intensities, network dimensions, as well as the node deployment densities. The purpose of this evaluation is to study the effectiveness of the detection scheme in the presence of varying numbers of attacker nodes, under different sensor network-application scenarios. We studied the energy decay rates of the GN, mGN, and the target nodes for varying applications of the sensor networks (varying α and (Δ_{opt}), the attack detection rates of the scheme for variations in several parameters, the effect of the threshold subpattern update rate on the detection process, based on expected network traffic, as well as the actual observed traffic, the false alarm rates of the detection scheme, for variations in the network parameter values, and the attack traffic intensities, the experimental results generated from a SOM- based, centralized approach for detection of distributed denial of service attack patterns. The outcomes of this experiment were studied to prove the need for having a distributed pattern recognition mechanism in place to detect distributed denial of service attacks in wireless sensor networks, which is achieved through the distributed detection scheme. we compared the performance of the two approaches, in terms of the metrics defined above. The contributions of this work are as follows:

We measured the performance of our scheme based on the following metrics:

- Attack detection rates.
- False positive rates.
- False negative rates.
- GN and mGN node energy decay rates.

We tested the effectiveness of the proposed scheme for variations in the following algorithmic and network-level parameters:

- Number of detector nodes (*n*).
- Network traffic intensities (adversarial nodes).
- Node deployment densities.

We proved the superiority of our proposed distributed pattern recognition scheme over a centralized Self Organizing Map-based approach, for variations in all the above parameter values.

III. Results and Discussion

Wireless sensor networks are deployed for specific sensing and reporting applications. The area of sensor node deployment depends on the nature of the application, and the total number of nodes to be deployed depends on several characteristics of the application, namely, expected node lifetimes, expected per-node load and node sensing ranges. Generally, most networks studied span a two dimensional area of size 100m x 100m (13). In a 200m x 200m network is considered to study a centralized data gathering and communication mechanism, based on an ant colony optimization algorithm. In (14), a 50m x 50m area is simulated to study a novel algorithm for code propagation in wireless sensor networks. All the above networks are considered with variations in the total numbers of nodes deployed. The average number of nodes in the network depends on the communication range of individual sensor nodes, as well as the topological specifications of the network. For large dimension networks, either sensor nodes with strong communication antennas need to be implanted, to facilitate direct node-base station communication, or a multi-hop topology needs to be in place for data delivery. Although most sensor networks studied in the literature have less than 500 nodes, we intend to study the effectiveness of our scheme in the presence of a large set of sensor nodes, and its impact on the overall success in attack detection. We perform experiments for varying node deployment densities on a 100m x 100m network. The values of the node deployment density, denoted as *N*, are: 128, 256, 512, 1024 and 2048. The simulation experiments are performed for two types of adversarial nodes, namely, injected nodes and laptop-class nodes. It is assumed that all nodes are equally likely candidates for loss owing to failures, battery exhaustion or compromise. The GN and mGN nodes in the network participate in routine sensing operations, in addition to participation in the attack detection process. Therefore it may be safely presumed that the task of selectively identifying and launching attacks against such nodes by the adversary-class is nontrivial. We also assume that sensor nodes have a single interface for both transmit and receive operations. We consider a standard sensor node with average energy consumptions for transmission and reception as: E_{trans} = 100 nJ/bit and E_{recv} = 50 nJ/bit, respectively (15). We also assumed that a typical sensor node has a maximum radio range of 50 meters (16).

The following parameters were incorporated in the simulation setup for the scheme:

- *SR*: The transmission range of a sensor node » 50m.
- Δ_{opt}: Time epoch length for detection scheme convergence (Calculated based on Equation).
- α: Application aspect value.
- *TI*: Traffic intensity in terms of packets/second.

- *TIe* (Traffic Intensity): Packets generated towards the *r* target nodes during a given time epoch (Δ_{opt}), in terms of energy resource usage by the target nodes.
- Number of Target nodes: *r* = 10% of *N*.
- Number of Detector (GN) nodes: *n*.

If the current epoch of time is defined as ¢*i*, then the subsequent epoch of time, based on Lemma is given by:

$$\Delta_{i+1} = \Delta_i + \Delta_{opt}.(3.d3 + \frac{n}{m}.d2\text{-}1 + m.d1) \qquad (3.1)$$

Where,
d1 = Average GN to GN communication delay
d2 = Average GN to mGN communication delay
d3 = Average mGN to BS communication delay

The time epoch length is dimensionalised into the unit of time (seconds), and is large enough to accommodate the entire communication phase of the attack detection scheme. For each value of *N*, we generate simulation plots for varying intensities of traffic generated in the network. These traffic intensities, denoted as *TI*, are inclusive of both normal and attack traffic. For a standard sensor network, the frequency of packet arrivals at a particular node depends on the node's topological placement in the network. For a network with *N* = 1024, with 10 operational cluster heads, the total number of packets expected by each cluster head during a given time epoch, is approximately equal to 100 sensory packets, for a network with a constant taxonomy i.e. 1 packet generated by every node per time epoch, for delivery to the cluster head. Therefore, a standard cluster head receiving in excess of 100 packets per time epoch, can be considered to be under attack. We define *TI* = 500 packets/sec, for a scenario with time epoch = 1 second, as network traffic with unusual intensity, intended to flood a victim node, and exhaust its limited energy resource. The traffic arrival rate is modeled as a Poisson process with exponential inter arrival times. The convergence phase of the scheme is the time required to execute the communication phase of Algorithm, wherein the GN and the mGN nodes perform pattern reconstruction, by exchanging subpattern values amongst themselves, to confirm an attack.

3.1 Energy Decay Rates

As described, the application aspect value, *α*, is a system parameter defining the significance of the accuracy in attack detection over the energy utilization rates of the GN/mGN nodes or vice versa. The normalized value of *α* between *f*0.0-1.0*g* is defined at network initialization time. The value of the parameter *k* of the *mSelect* algorithm is inversely dependant on the selected value of *α*. Large values of *α* signify the need for achieving higher accuracies in attack detection. Therefore, selection of a large *α* value (close to unity) will generate smaller values for the parameter *k*, of the *mSelect* algorithm, effectively leading to the designation of a large number of mGN nodes for the detection scheme. Similarly, smaller values of *α* will lead to the generation of higher values of *k*, and in essence will lead to fewer numbers of mGN nodes in the network.

In Figure 1, we illustrate the overall energy consumption rates of the GN nodes of the network. The energy consumption rates of the GN nodes increase with corresponding increases in the value of *α*. For instance, for *N*=128 and *α*=0.1, the energy consumption is at 51 ^{1}J/sec, whereas for *α*=0.9, the nodes utilize 84 ^{1}J/sec. This increase in the energy consumption of the GN nodes for higher *α* values is attributed to the corresponding decrease in the size of the time epoch length Δ_{opt}, for achieving higher accuracies in the attack detection rates. It may be noted here that increasing values of *N* lead to improved energy consumption rates for individual GN nodes, as the proximity of the GN nodes leads to reduced communication distances that need to be traversed by the GN communication messages.

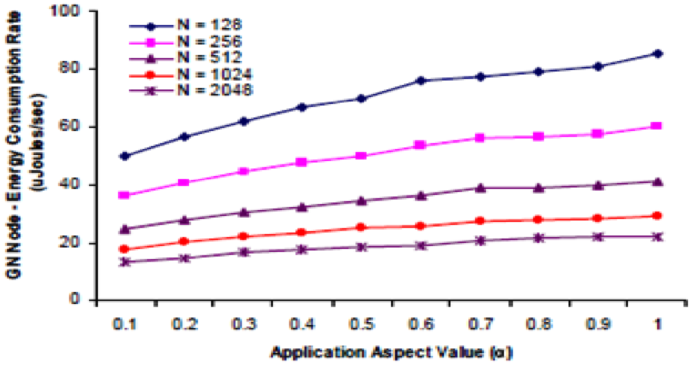

Figure 1: GN Node Energy Utilization Rate vs. Application Aspect Value (*α*).

The peak energy consumption rates in μJ/sec (α = 0.1) is 86 for N=2048. The energy consumption rate of 17 μJ/sec is lowest for α=1.0 and N=128.

We illustrate the energy consumption rates of the mGN nodes of the detection scheme in Figure 2. For all node deployment densities, the mGN nodes can be seen to consume more energy than the GN nodes. This is due to the additional tasks imposed on the mGN nodes for message reception, analysis, and delivery to the base station, as compared to the standard tasks of a GN node, which involve observation and reporting of traffic flow data to a closely located mGN node. The mGN nodes show a decrease in the energy consumption rate for corresponding increases in the value of α. This trend occurs due to the reducing number of mGN nodes selected for the attack detection process, for decreasing values of α. Therefore, the energy consumption rate for N=2048 and α=0.1 is close to 360 μJ/sec, whereas for α=0.9, it is only 126 μJ/sec. For lower values of N, the energy consumption rate of the mGN nodes is lower; as fewer number of GN nodes will collaborate with their designated mGN nodes, and therefore will lead to lesser energy utilization rates. However, even for lower values of N, the overall energy consumption rate of the mGN nodes reduces with increasing α.

For low node deployment densities, the energy consumption rates of the mGN nodes are higher, as compared to networks with higher values of N. Communications over longer distances that need to be performed in less dense networks lead to higher energy utilization rates for lower N. For N=128 and α =0.1, the mGN nodes consume 126 μJ/sec, whereas, for N=2048 and α=0.1, the mGN nodes consume 360μJ/sec. Similarly, for N=128 and α =0.1, a GN node will consume 21 μJ/sec, whereas for N=2048 and α =0.1, the energy consumption rate of a GN node is 84 μJ/sec. For higher node deployment densities, more numbers of GN nodes communicate with each mGN node. Therefore, the overall energy consumption rate of the mGN nodes depicts an increase for corresponding increase in the value of N. In Figure 3, we illustrate the total number of mGN nodes selected by the *m*Select algorithm for varying values of α and N. As can be observed, for lower values of α, the total number of mGN nodes selected is very low. For instance, for N=128 and α =0.1, the total number of selected mGN nodes is 2. Smaller values of α imply lesser significance on the accuracy in attack detection, and more significance applied to the energy conservation of the GN and mGN nodes.

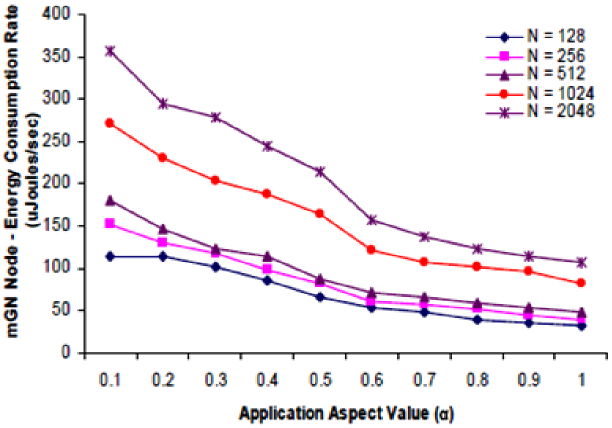

Figure 2: mGN Node Energy Utilization Rate vs. Application Aspect Value (α).

The peak energy consumption rates in μJ/sec (α = 0.1) is 352 for N=2048. The energy consumption rate of 32.3 μJ/sec is lowest for α =1.0 and N=128. Therefore, the detection rate accuracy, affected by the longer convergence delays associated with the *communication* phase of the attack detection process (as each node has a single interface for message transmission and reception), has a corresponding energy conservation factor associated. Similarly, higher values of α imply more significance given to the accuracy in attack detection as compared to the energy conservation of the GN/mGN nodes. In such scenarios, more number of mGN nodes are selected by the *m*Select algorithm, so as to reduce the convergence delays of the attack detection scheme, effectively increasing the attack detection rate. However, as illustrated in Figure 2, the higher energy consumption rates of the mGN nodes will lead to rapid reduction of their respective lifetimes.

Considering the significantly high energy utilization rates of mGN nodes as compared to the GN nodes, the presence of a large number of mGN nodes will incur significant overhead on the network, and will lead to reduced lifetimes of a larger number of sensor nodes. Therefore, from an energy consumption perspective, the fewer the number of mGN nodes, the longer the lifetime of the sensor network. The set of mGN nodes for the detection scheme are selected based on Algorithm, which operates by reducing any redundancies in node selection.

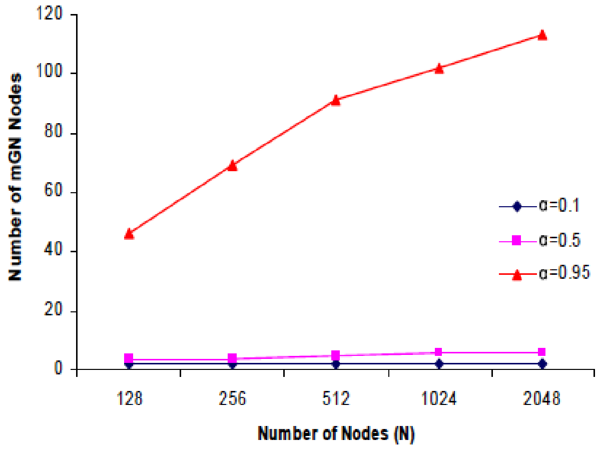

Figure 3: Number of mGN Nodes vs. Total Number of Nodes.

The peak energy consumption rates in ^{1}J/sec (® = 0.1) is 86 for *N*=2048. The energy consumption rate of 17 ^{1}J/sec is lowest for ®=1.0 and *N*=128. In Equations 5.2 and 5.3, we define the standard energy decay rates for a GN and an mGN node, per time epoch of length Δ*opt*. Each GN node receives exactly two traffic observation packets from its neighboring GN nodes within each time epoch. Therefore, the energy associated with receiving packets, is given by: 2.E_{recv}. In addition, the GN nodes monitor traffic flow in the network. The total energy usage associated with receiving all packets in a single epoch of time is given by: 2.*Erecv* + *pkts*(*obsv*).*Erecv*. Each GN node communicates with exactly three other nodes, namely, two peer GN nodes, and one mGN node, during each time epoch. Considering the average distance between any two GN or mGN nodes to be $d_{GN\text{-}mGn}$, the energy usage associated with the transmission of data by a GN node in a single time epoch, is given by: 3.*Etrans*.$d_{GN\text{-}mGn}$.

The mGN nodes receive packets from *n*/ *m* - 1 GN nodes within each time epoch. They are also responsible for transmission of one packet to the base station, located at an average distance of $d_{mGn\text{-}BS}$. The total costs of receiving and transmitting data packets by the mGN nodes are given by:[(*n*/*m*-1).*Erecv*] and [E_{trans}.*d*4 $_{mGn\text{-}BS}$], respectively.

$$\mu_{gm}=\frac{2.Erecv+3.Etrans.d2GN-mGn+pkts(obsrv)Erecv}{\Delta opt} \qquad (3.2)$$

$$\mu_{mgm}=\frac{(\frac{n}{m}-1).Erecv+Etrans.d4mGN-BS}{\Delta opt} \qquad (3.3)$$

This value defines whether more significance is to be given to the conservation of energy of the GN and mGN nodes, or to the conservation of energy of the target nodes. Higher values of selected at network initialization time define the significance of conserving energy content of the GN and mGN nodes, over the quicker detection of an attack. On the contrary, lower values of define the significance of rapid attack detection, over the need for conservation of the energy content of the GN and mGN nodes.

The impact of the variation of the Δ*opt* value on the energy resource utilization of the detector as well as the mGN nodes, for a network with *N*=1024 and *TI* = 500, is illustrated in Figure 4. In addition, the figure also illustrates the rate of decay of the energy content of a target node under an attack (*TI*=500). The optimal length of a time epoch is computed based on Equation and is affected by the following network and algorithmic parameters: *n*, *N*, *m*, *TIe*, apart from the energy utilization rates, which are fixed system parameters.

The mGN nodes of the network participate in active reception of a large numbers of packets within each epoch of time, and are responsible for further forwarding of a verdict signal to a base station, over a longer communication channel. These tasks are performed by the mGN nodes, in addition to their detection tasks, as well as routine sensory operations. Therefore, the energy decay rates for mGN nodes are significantly higher as compared to GN nodes. Networks with low node deployment densities will have fewer numbers of nodes, with increased per-node overhead associated with the GN and varying values of Δ*opt*(seconds), *TI* = 500, *N*=1024.

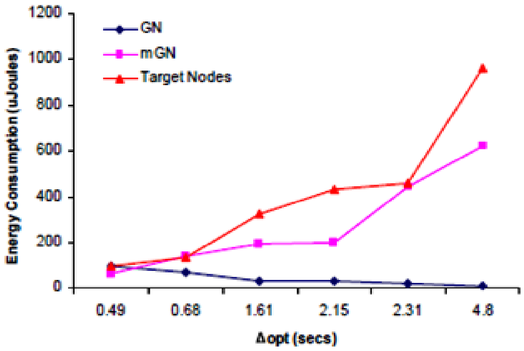

Figure 4: Energy decay rate of detector (GN), mGN and target nodes for mGN tasks.

On the contrary, networks with higher node deployment densities will have reduced dependence on a few select nodes, operating as mGN nodes. Therefore, higher node deployment densities will yield lower per-node overhead, associated with the mGN tasks. Higher node deployment densities will also increase the values of Δ*opt*, thus leading to less frequent convergence of the detection scheme, and lower energy decay rates for the GN and mGN nodes.

Larger values of Δ*opt* will cause the detection scheme to converge on a less frequent basis, and therefore will yield lower energy decay rates for the GN nodes. However, the increasing value of Δ*opt*, attributed to increasing values will lead to the selection of fewer mGN nodes in the network, and therefore, the per-mGN node energy consumption rate increases. Smaller values of Δ*opt* will lead to more frequent convergence of the scheme, and therefore higher energy consumption rates are observable for the GN nodes. For larger values of Δ*opt*, the target nodes under an attack will have a higher percentage of their energy content depleted before an attack against them is actually detected. For instance, for Δ*opt* = 4.8 seconds (α =0.1 and *TIe*=40), nearly 970 ^{1}Joules are consumed by the target node each second, as compared to 100 ^{1}Joules consumed, for ¢*opt* = 0.49 seconds (α =0.95 and *TIe*=400).

Increasing values of *k* (decreasing α), will lead to lesser overlaps in the *k*-lists of each of the GN nodes, exchanged with the base station at network initialization time. As a result, fewer number of mGN nodes are selected. The reducing number of mGN nodes lead to an increase in the per-mGN node energy utilization rate. Considering the high energy utilization costs associated with the mGN nodes, it is recommended to have as few mGN nodes operating in the network as possible. However, the accuracy in attack detection of the scheme will in effect diminish, as will be elaborated in the following subsection.

3.2Attack Detection Rates

The attack detection rate is defined as the ratio of the total number of attack packets classified correctly, over the total number of attack packets, given by:

Attack Detection Rate =Total Observed Attack Packets/Total Attack Packets (3.4)

In Figure 5, we analyse the effect of variation of the value of the application aspect value, α, on the attack detection rate. As seen from the figure, the attack detection rate is higher for ® close to unity. For instance, for α = 1.0, the attack detection rate is 38% for *N*=128, whereas, for α = 0.1, the detection rate is only 10%. For *N*=2048, the detection rate is 92% for α =0.1, and is 86% for α =1.0. A similar increase in the attack detection rate for increasing values of α is observable for the other node deployment densities.

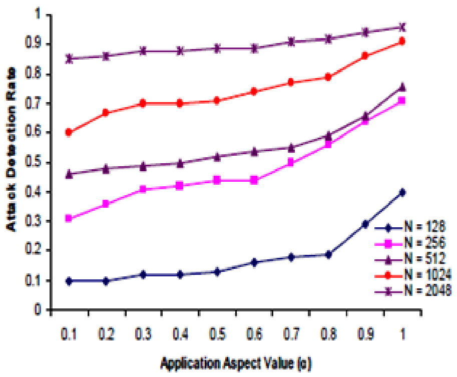

Figure 5: Attack Detection Rate vs. Application Aspect Ratio (α) for *TI* = 500.

The peak detection rate (α = 1.0) is 38% for *N*=128, 65% for *N*=256, 71% for *N*=512, 84% for *N*=1024 and 92% for *N*=2048. The detection rate is lowest for α =0.1: 10% for *N*=128, 31% for *N*=256, 47% for *N*=512, 61% for *N*=1024 and 86% for *N*=2048.

For purposes of our simulation experiments to compute the attack detection rate, false alarm rates and the time epoch length, we have considered the value of α to be 0.95, to study the peak accuracies in attack detection. In Figure 6, we illustrate the attack detection rate for a network with node deployment density, *N* = 128. The intensity of the total traffic in the network, inclusive of attack as well as normal packets, is varied from 50 packets/sec to 500 packets/sec. The total number of detector nodes (*n*) is also varied from 1% to 100%. For *TI* = 50, the detection rate reaches nearly 72%, when the number of detector nodes = 100%. Due to the low node deployment density of this network, the detector nodes in the network cannot reconstruct, in their entirety, accurate traffic observation patterns, as packets penetrating the network from unobserved regions of the network are not accounted for, by the detector nodes. Therefore, the detection rate does not cross 72%, even with 100% GN nodes in the network, and low traffic intensities.

For higher values of *TI*, the detection rates further degrade, with the detection rate being only 30%, for *TI* = 500 and *n* = 100%. This is because high *TI* values imply larger numbers of packets penetrating the network, whilst the attack detection scheme is still in the process of convergence. These packets remain unobserved by the detector nodes, and thus the performance of the scheme in terms of the detection rates, degrades with increasing traffic intensities.

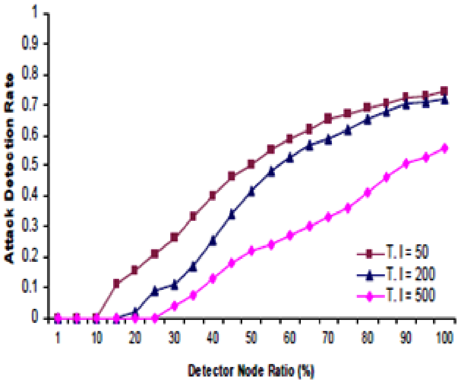

Figure 6: Attack Detection Rate vs. Detector Node Ratio for *N* = 128.

The peak detection rate is approximately 72% for low traffic intensity and *n* = 100%. For *n* < 10%, the detection rate is negligible for all traffic intensities.

For the *N*=256 scenario (Figure 7), smaller values of *T:I:* require fewer numbers of active detector nodes in the network for reaching higher attack detection rates. For *T:I:*=50, with roughly 35% detector nodes, the detection rate is nearly 53%, as compared to the *N*=128 scenario, where the detection rate was less than 33%. The increase in the densities of nodes deployed in the network improves the chances of detector node presence in all regions of the network. As a consequence, higher detection rates are witnessed for fewer number of operating detector nodes. For larger values of *TI*, the scheme shows good improvements over the *N*=128 scenario, with the detection rate approaching nearly 70% for *TI*=500, as compared to *N*=128, where the detection rate did not exceed 33%, for the same traffic intensity. Larger numbers of detector nodes in the network facilitate the verification and reconstruction of a pattern depicting observed network traffic, with higher degree of accuracy. Therefore, higher detection rates are observed.

In the *N*=512 (Figure 8) scenario, attack detection rates peaked to nearly 90% in the presence of as few as 20% detector nodes in the network. The higher density of node deployment in these networks, assure that fewer detector nodes are required to achieve higher success in the attack detection process. This is because the higher numbers of detector nodes in the network help accurately reconstruct traffic observation patterns, from individual readings of the large number of attack detector nodes, thus leading to higher detection rates. The parallel nature of execution of the communication phase of the detection scheme, wherein the GN and mGN nodes coordinate to reconstruct the complete pattern of observed traffic, reduces the overhead associated with having higher number of detector nodes on the convergence delay of the detection scheme.

Again, higher values of *TI* yield lower attack detection rates, when fewer numbers of detector nodes are operational in the network, for this network scenario, with *TI*=500 yielding a detection rate of 82%, with *n* = 100%. This is because of the larger numbers of attack packets penetrating the network, and remaining undetected, during the convergence of the communication phase of
the detection scheme.

In the *N*=1024 scenario (Figure 9), lower values of *TI* require fewer number of active detector nodes in the network for reaching relatively high attack detection rates. For *TI*=50, with *n*=22%, the detection rate is nearly 93%.

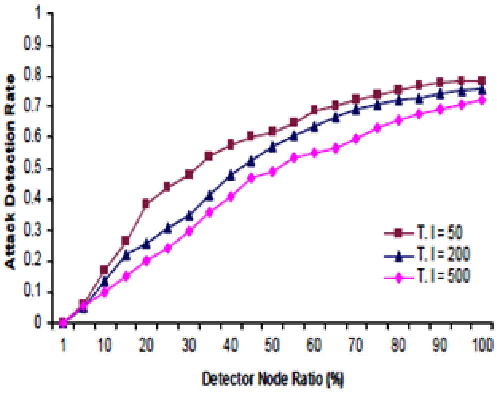

Figure 7: Attack Detection Rate vs. Detector Node Ratio for *N* = 256.

The detection rate approaching 70% even with high traffic intensities (*TI*=500), and fewer than 100% *n* nodes required to attain high detection rates.

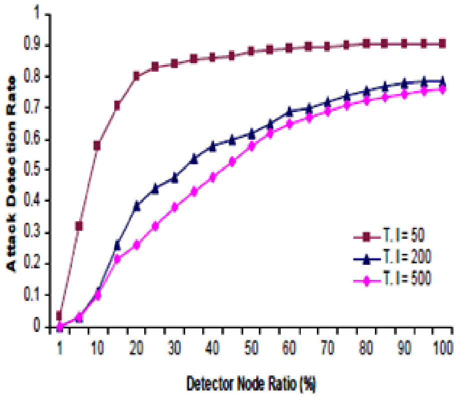

Figure 8: Attack detection vs Detector node ratio

The increasing densities of node deployment improve the chances of detector node presence in all regions of the network. As a consequence, very high detection rates are witnessed for fewer number of operating detector nodes. The expected performance improvements owing to the participation of a larger set of detector nodes in the detection process, is subdued for higher values of *TI*. For *TI* = 500, the detection rate is nearly 82%, with 100% detector nodes, whereas for *TI*=50, the detection rate is as high as 96%.

However, for larger values of *TI*, the scheme shows reasonable improvements over the previous network scenarios, with the detection rate crossing the 80% mark for *n* = 100% for *N*=1024, as compared to all the previous network scenarios, *N*=128, 256 and 512.

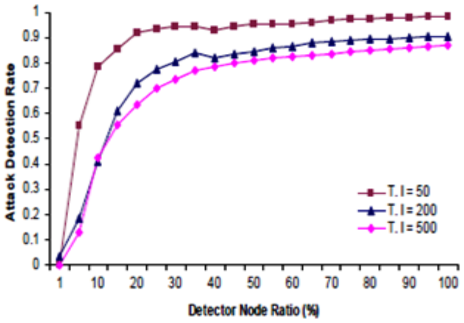

Figure 9: Attack Detection Rate vs. Detector Node Ratio for *N* = 1024.

Peak detection rate of 93% for low traffic intensities. Even high values of *TI* yield a detection rate of above 80% for higher *n*.

The detection rates for the *N*=2048 scenario (Figure 5.10) are the best amongst all networks. This is because of the ability of the detection scheme to accurately reconstruct traffic observation patterns, even in the presence of high traffic intensities. We can observe a detection rate of nearly 97% for as few as 50% detector nodes, and *TI*=50, and approaches nearly 90% for *TI*=500.

In Figure 5.11, we illustrate the effect of the variation of the detector node ratio on the attack detection rate for various node deployment densities. For lower values of *n*, very high density networks can sustain a reasonable detection rate. As can be observed, *n*=0.05*N* yields a detection rate of only 40% with *N*=2048. Increasing values of *n* yield higher detection rates for all node deployment densities, with *n*=0.75*N* performing nearly as good as the *n*=*N* scenario, for *N*=2048. It may be conjectured that the need for having all nodes operating as detector nodes is not essential, if the node deployment density of the network is high. However, the detection rate improvements are reasonably higher for less dense networks, with higher values of *n*.

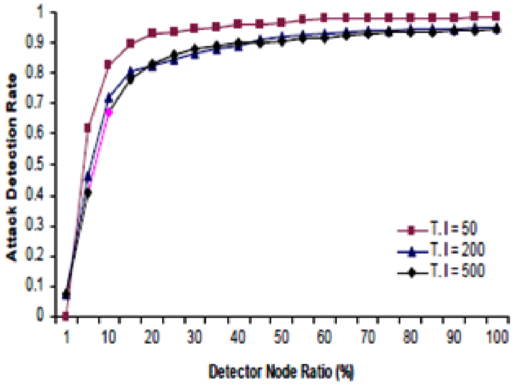

Figure 10: Attack Detection Rate vs. Detector Node Ratio for *N* = 2048.

Peak rate of 97% for low traffic intensities. Only 10-15% of detector nodes needed to achieve high detection rates.

IV. Conclusion

The fewer numbers of detector nodes in the network will lead to the reconstruction of less accurate patterns, to depict actual network traffic flow. This phenomenon occurs because of the inability of the scheme to perform attack detection in the presence of unobserved regions of the network under a distributed denial of service attack. A centralized attack scenario will yield comparable detection rates for both low as well as high density networks. We may therefore conclude that higher densities of node deployment yield higher attack detection rates, for fewer numbers of operational detector nodes. We may also infer that higher values of *TI* will lead to lower detection rates, due to the larger numbers of attack packets penetrating the network, unnoticed, whilst the scheme communication phase is still converging. The parallelism in the execution of the GN pattern reconstruction process (Communication phase of Algorithm), helps improve detection rates with corresponding increases in the value of *n*, thus proving the scalability of the detection scheme for denser networks.

References

[1]. Jalili, R., Imani-Mehr, F., Amini, M. and Shahriari, H. (2005). Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks, *In Proc. of the First Information Security Practice and Experience Conference*, pp. 192-203.

[2]. Gligor, V. D. (1984). A note on the denial-of-service problem, *IEEE Trans-actions on Software Engineering* 10(3): 320-324.

[3]. Jung, J., Krishnamurthy, B. and Rabinovich, M. (2002). Flash crowds and denial of service attacks: Characterization and implications for cdns and web sites, *In Proc. of the Intl' World Wide Web Conference*, pp. 252-262.

[4]. Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D. and Pister, K. (2000). System architecture directions for networked sensors, *Acm Sigplan No- tices* 35(11): 93-104.

[5]. Intanagonwiwat, C., Govindan, R. and Estrin, D. (2000). Directed discussion: A scalable and robust communication paradigm for sensor networks, *In Proc. of the Sixth Annual Intl' Conf. on Mobile Computing and Networks (MOBICOM'00)*, pp. 56-67.

[6]. Gligor, V. D. (2003). Guaranteeing access in spite of service-flooding attacks, *In Proc. of Intl' Workshop on Security Protocols*, pp. 80-96.

[7]. Izhikevich, E. (1999). Weakly pulse-coupled oscillators, fm interactions, synchronization, and oscillatory associative memory, *IEEE Transactions on Neural Networks* 10(3): 508-526.

[8]. Ghosh, A. and Schwartzbard, A. (1999). A study in using neural networks for anomaly and misuse detection, *In Proc. of the Eigth USENIX Security Symposium*, pp. 12-12.

[9]. Hu, Y. C., Perrig, A. and Johnson, D. B. (2002). Wormhole detection in wireless ad hoc networks, *Technical Report TR01-384*, Rice University Department of Computer Science.

[10]. Javitz, H. and Valdes, A. (1991). The sri statistical anomaly detector, *In Proc. of the IEEE Symposium on Security and Privacy*, pp. 316-326.

[11]. Jin, S. and Yeung, D. (2004a). A covariance analysis model for ddos attack detection, *In Proc. of the IEEE Intl' Conf. on Communications*, pp. 1882-1886.

[12]. Jin, S. and Yeung, D. (2004b). Ddos detection based on feature space model-ing, *In Proc. of the Third Intl' Conf. on Machine learning and Cybernetics*, pp. 4210-4215.

[13]. Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J. and Silva, F. (2003). Directed distribution for wireless sensor networking, *IEEE/ACM Transactions on Networking* 11(1): 2-16.

[14]. Hussain, A., Heidermann, J. and Papadopoulos, C. (2003). A framework for classifying denial of service attacks, *In Proc. of the ACM SIGCOMM 2003*, pp. 99-110.

[15]. Karlof, C. and Wagner, D. (2002). Secure routing in wireless sensor networks: Attacks and countermeasures, *In Proc. of the First IEEE Intl' Workshop on Sensor Network Protocols and Applications*, pp. 113-127.

[16]. Gligor, V. D. (2004). Security of emergent properties in ad-hoc networks, *In Proc. of Intl' Workshop on Security Protocols*, pp. 256-266.