Intrusion Recovery Framework for Tactical Mobile Ad hoc Networks

Sathish Kumar P. Alampalayam[1], S. Srinivasan[2]
[1]Computer Science and Information Technology Department
PSG Institute of Advanced Studies, Coimbatore – 641004, India
[2]Computer Information Systems Department
University of Louisville, Louisville, KY 40292, USA

Summary
Mobile ad hoc networks (MANET) are infrastructure free networks, temporary in nature and without any centralized authority. These unique characteristics, coupled with the increased vulnerability of MANET for security attacks, demand an immediate solution for securing the ad hoc network prior to its full-fledged deployment in commercial and military applications. So far, most of the research in MANET has been primarily focused on the routing and mobility aspects rather than securing the ad hoc networks. Due to the ever increasing security threats, there is a need to develop architecture, algorithms, and mechanisms for a secured ad hoc network infrastructure. Existing Intrusion Detection Approaches (IDA) in MANET suffer from the lack of design and implementation details for intrusion response. To address this limitation, in this paper we are proposing an intruder identification and response framework for MANET. Experimental results of the model simulated in NS2 for selected Denial of Service attacks are very promising.

Key words:
Mobile Ad hoc Networks, Intruder identification, Response actions, NS2, Denial of Service attacks

1. Introduction

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority. In a MANET, the nodes are free to move about and organize themselves into a network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. For instance, MANET can be used by first responders at a disaster site or soldiers in a battlefield to provide their own communications.

Until recently, the main research focus has been on improving the protocols for multi-hop routing, performance and scalability of the ad hoc networks [1]. Though the performance and scalability have their place in wireless and tactical MANET research, the current and future applications of the ad hoc networks has forced the research community to look at dependability and security aspects of ad hoc networks. Security in mobile ad hoc network is essential even for basic network functions like routing which are carried out by the nodes themselves rather than specialized routers. The intruder in the ad hoc network can come from anywhere, along any direction, and target any communication channel in the network [1]. Intrusion prevention techniques such as authentication and encryption are applicable in the wired and infrastructure-based cellular network. In the case of infrastructure-free mobile ad hoc networks these techniques are not applicable [3]. The dynamic nature of the ad hoc network also means that trust between nodes in the network is virtually non-existent. Without trust, preventive measures are unproductive and measures that rely on a certain level of trust between nodes are susceptible to attacks themselves. Hence there is a need for intrusion detection and response since it provides a second line of defense.

Intrusion detection is the process of detecting and responding to malicious activity that is aimed at attacking the network [3]. Several techniques for detecting intrusions have been studied. An overview of the existing IDA techniques can be found in [3-8, 17-21]. There are several weaknesses in the current IDA applied to MANET [3-8]. The most important among them is the lack of intrusion response to identify the intruder and respond to the attack and ensure safety of the MANET once an attack is detected. Although intrusion response framework is related and coexists with the intrusion detection framework, it receives considerably less attention than IDA owing to the inherent complexity in developing and deploying response in an automated fashion. As such, traditionally, triggering an intrusion response is left as a part of the administrator's responsibility. In the context of MANET, we need to identify the intruder and take a proper evasive or corrective action to isolate the intruder from the network and protect the MANET. This paper addresses such counter measures referred to as Intrusion Response Approach (IRA).

Intrusion Response Approaches

IRA can be classified as follows [13]:

Passive response vs. Active response:

Manuscript received September 5, 2009
Manuscript revised September 20, 2009

Passive response systems do not attempt to minimize damage already caused by the attack or prevent further attacks. Their main goal is to notify the authority and provide the attack information. Active responses on the other hand aim to minimize the damage done by the attacker and attempt to locate or harm the intruder [13]. Our model is based on active response approach since it identifies the intruder and mitigates the attack by isolating the intruder.

Manual response vs. Automatic response:

Manual response approaches provide lower degree of automation than automatic response approaches but they provide higher degree of automation compared to notification-only approach. Automatic responses provide immediate response to the intrusion through automated decision making process [13]. Although intrusion detection systems are greatly automated nowadays, automatic intrusion response support is still very limited. Our model is based on automatic response due to automated decision making process.

Static response vs. Adaptive response:

Majority of the IRA are static due to the reason that the response selection mechanism remains the same during the attack period. These systems can be periodically upgraded by the administrator; however, such support is manual. Although this approach takes a conservative view of the system and environment, it is simple and easy to maintain. Adaptive responses on the other hand dynamically adjust response selection to the changing environment during the attack time [13]. Adaptation mechanism can be represented in several ways: (a) adjustment of system resources devoted to intrusion response such as activation of additional IDS, or (b) consideration of success and failure of responses previously made by the system. Our approach is based on static response.

Proactive response vs. Delayed response:

Proactive response approach allows foreseeing the incoming intrusion before the attack has affected the resource. Such prediction is generally hard and often relies on the probability measures and analysis of current user/system behavior. Proactive nature of the response also requires that the detection and response frameworks are tightly coupled such that responses can be fired as soon as a likelihood of attack is identified. Although proactive detection of the attack and early response is a desired feature, it is often hard to guarantee 100% correctness of the triggered action. In the Delayed response approach, response action is delayed until the attack has been confirmed. Such assurance may be provided through the confidence metrics of IDS. Our approach is based on delayed response since the responses are fired as soon as the attack is detected.

Independent response vs. Cooperative response:

Independent response approach handles intrusion independently at the node it was detected. A host-based IDS detecting an intrusion on a single machine will trigger a local independent response such as terminating a process or shutting down the host, etc., Cooperative response approach refers to a set of response systems that combine effort to respond to an intrusion [13]. Cooperative approach consists of several independent approaches that are capable of detecting and responding to intrusions locally; however, the final strategy is determined and applied globally. Since network-based IDS are built in such a cooperative manner, our model has a cooperative response approach.

In this paper, we propose an automated framework that can identify the intruder through the audit data and respond to the intruder through corrective response action plans and protect the MANET. The paper is organized as follows: Section 2 summarizes the existing intrusion response approaches for MANET and their limitations. Section 3 describes our MANET intruder identification and response framework with its architecture and mechanism. Section 4 presents an overall algorithm for the intruder identification and response framework. Sections 5 and 6 present the example and mathematical analysis for the framework, respectively and Section 7 explains the experimentation and simulation carried out in MANET using NS2 to demonstrate the validity of the intruder identification and response framework for MANET. Section 8 presents the conclusion.

2. Related Work

2.1 Related Intrusion Response Approaches in MANET

There are very few IDA models that provide the integrated detection and response feature. Zhang et al., in their framework have explained that local response module triggers action local to the mobile node and the global response module coordinates actions among neighboring nodes, such as the IDS agents in the network electing a remedy work [3]. They have also explained that the type of response depends on the type of intrusion, the type of protocols, applications and the confidence in the evidence with examples. However, they have not provided any implementation details regarding the intrusion response aspect of the model. Similarly, there is no documentation on the simulation or experimental results on the response aspect of the model. However, there is a detailed explanation on the experimental results of the

intrusion detection mechanism. Thus, even though the idea of integrated detection and response model seems feasible, it appears that the implementation and simulation have not been conducted. Similarly, few related IDA models propose response actions/frameworks for responding to the attacks once it is detected [3-8]. However the response system incorporating all those actions is not implemented.

There are only a few intrusion prevention approaches described in the literature for MANET security. Puttini et al [9], have proposed a secure routing protocol that combines a certificate based authentication service with intrusion detection model to provide preventive and corrective protections for MANET. Bhargava [10], have proposed a security model for AODV routing protocol.

2.2 Limitations of existing Intrusion Response Approaches

It can be noted that though the response concepts are explained in the existing intrusion detection models, implementation details and results for the response framework are not provided to demonstrate and validate their response techniques [3-10]. Also, according to our literature review, we observe that none of the existing models has proposed an intrusion control approach for MANET such that detection and response are done continuously to protect the MANET [3-10].

The current schemes thus have practical problems in real time response. The proposed Intrusion identification and response framework for MANET addresses many of these limitations. Our model continuously monitors the online network data and efficiently identifies the intruder and responds to the attacks.

3. Security Model Architecture

The proposed security model uses a feedback control scheme that is analogous to the human biological model wherein an attack is detected by measuring body parameters like temperature, blood sugar and blood pressure level and comparing them against their normal values. Once an attack on the body is detected, it is treated to bring the body to the normal state. Similarly, in this security model various parameters of an ad hoc node or a set of ad hoc nodes are monitored. If these parameters change rapidly in a given time frame, the appropriate threat is detected, intruder is identified and a corrective action is taken. The proposed framework is a centralized model. All the nodes in tactical ad hoc network need to run cooperatively to make the framework applicable.

In the Figure 1, tactical MANET is represented as a function: $f(x_1(t), x_2(t),\ldots x_n(t), v_1(t), v_2(t)\ldots v_n(t), m_1(t), m_2(t),\ldots m_n(t), k(t), u(t))$, where $x_n(t)$ represents the significant attack sensitive network parameters, $v_n(t)$ represents the network parameters which are not significant in representing the node vulnerability, $m_n(t)$ represents the mobility parameters, k(t) represents the attack and u(t) represents the control input. $x_n'(t)$ represents the modified values of the significant attack sensitive network parameter due to the influence of the attack k(t) and the control input u(t). Threat Index (TI) for a node is calculated by the detection framework from the attack sensitive network parameters, $x_n'(t)$ using fuzzy logic [16]. The computed Threat Index TI(t) is compared with the threshold values of the Threat Index TI'. The Threat Index thresholds (TI') are obtained with the help of the training dataset where the state of each record is labeled. Data records collected from simulation environment with and without attack are used as training dataset for identifying the Threat Index thresholds. As shown in Figure 1, the training data is derived from the MANET and is used in the identification of significant parameters and the thresholds of these parameters and the threat index. If the computed TI(t) of a node is greater than or equal to vulnerable state threshold reference TI', the node is identified to be under threat. Upon detecting that a node is under threat, the neighboring nodes are subjected to the response and protection algorithm in the response framework. This response algorithm identifies the intruder and sends the control signal u(t) to isolate the intruder from the MANET. The control signal u(t) varies depending upon the type of the intrusion. The different types of control actions are explained in the following sections. This control signal reconfigures the MANET and modifies $f(x_1'(t+1), x_2'(t+1),\ldots x_n'(t+1))$ such that TI(t+1) reaches the steady normal state. It should however be noted that $f(x_1'(t+1), x_2'(t+1),\ldots x_n'(t+1))$ also depend on any new attack k(t+1). This paper and the following experiments describe in detail the intruder identification and response framework of the model. The significant parameter identification, threat index calculation and intrusion detection aspect of the model was dealt in detail in our earlier work [15, 16]. With the help of dataset derived from MANET simulation, the approach from [15] was used in this paper and not the DARPA dataset explained in [15]. Syn flood DoS attack was applied in the simulations explained in Section 7. The proposed method will work for other kind of DoS attacks.

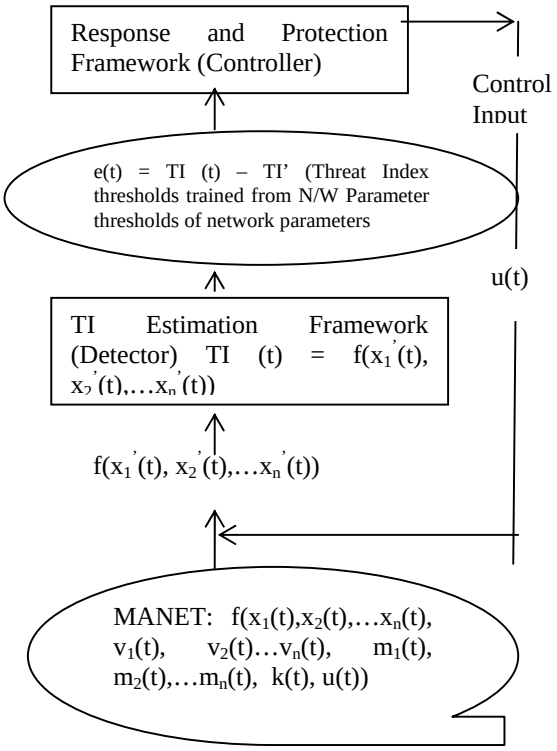

Figure 1 Feedback Control based Security Model

3.1 MANET Intruder Identification and Response Framework

This section explains the proposed intruder identification and response framework for MANET. The proposed framework is a decentralized model. All the nodes in tactical ad hoc network need to run cooperatively to make the framework applicable. The response and protection mechanism gets triggered when an attack is detected by the detection framework [2]. The response and protection framework identifies the intruder and responds to the attack with the response action plan. The significant parameters and their thresholds used for threat detection in the detection framework are used by the response and protection framework as well [2]. When the detection framework detects an attack, each neighboring source node to the node under threat is examined by the response framework, and different action plans are initiated based on the identification of the nature of the neighboring nodes.

Monitoring significant parameters is the starting point of the response framework architecture. "Monitor Significant Parameter" block in the response framework monitors significant parameters in each network node in a distributed and cooperative manner and feeds the collected observation to the "Reputation Management Mechanism" block. "Reputation Management Mechanism" block then updates the node's reputation rating counter. The term 'Reputation Management' in the architecture refers to assigning counters and flag to the nodes based on their behavior, which is achieved by monitoring significant parameters in a node level at a given instance. The reputation counter is updated by comparing the values of the significant parameters against an expected norm. The functionality of Reputation Management block is described using an example in section 5.

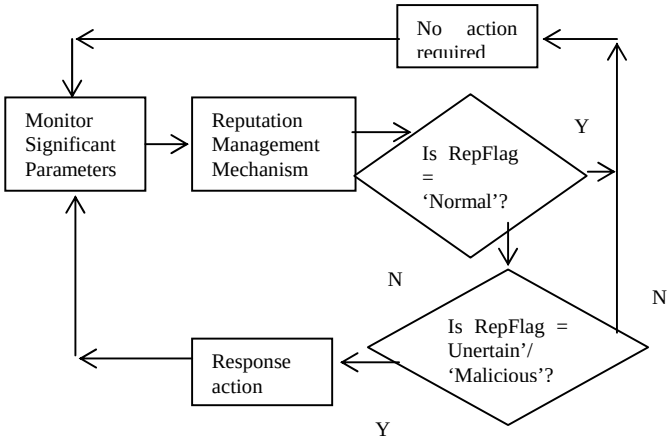

Figure 2 Architecture of the intruder identification and response framework

3.2 Intruder Identification Mechanism

Counters and flag are associated with each neighboring source node to the node under attack to implement the intruder identification mechanism for the response and protection framework. Each node has three types of counters – normal, uncertain and abnormal counter; the flag at each node can take three different values – normal, uncertain and malicious; the nature of the neighboring node is indicated by the value that its flag takes. For each node which is a neighbor to the node under attack, the response and protection mechanism compares the value of the significant attack sensitive network parameters with the uncertain state and vulnerable state threshold values and updates the counters. The normal counter is incremented when the value of a significant parameter falls in the normal range, the uncertain counter is incremented when a significant parameter takes a value in the uncertain range and the abnormal counter is incremented when a significant parameter value is in the vulnerable range. Since all the significant parameters that are selected have equal importance, they have equal

weight in the intruder identification and response mechanism. After the counters are incremented, the flag for the node is asserted using the following logic: If the value of the normal counter is greater than sum of the uncertain and abnormal counters, "normal" flag is asserted. If the value of the uncertain counter is greater than the sum of normal and abnormal counters, "uncertain" flag is asserted. If the value of the abnormal counter is greater than the sum of normal and uncertain counters, "malicious" flag is asserted. If all the counter values are equal, the "uncertain" flag is asserted. Based on the flag that is asserted, different response action plans are triggered. The response action plans are explained in the following subsection.

3.3 Response Action Plans

Response actions are required when the flag of a neighboring source node is "uncertain" or "malicious". The following action plans are used in the response framework.

Action Plan 1: If a neighboring source node to a node under threat is flagged as "normal", no action is needed since the node is neither malicious nor selfish. For this level, the following could be executed [11].

- Basic computer security policy like basic encryption, authentication, authorization.
- Specially designed core software for proactive security.
- Set the maximum concurrent connections allowed per user.
- Set the bandwidth at a lower acceptable level than the possible maximum.

Action Plan 2: If a neighboring source node to a node under threat is flagged as "uncertain", necessary precautions are needed to prevent further damage. In this case the following action plans could be executed:

- This plan executes moderate response action like automatic node re-authentication.
- Verify the correct execution of the packet forwarding function.
- Automatic modification of the routing table information to the original state
- Automatic modification of the propagation limits of the ad hoc nodes, in order to perform the packet forwarding function.
- Ability to drop idle connections.
- Filter "redundant" data packets or using routing information (filter spoofed packets traveling unexpected routes from their specified addresses) [11].

Action Plan 3: If a neighboring source node to a node under threat is flagged as "malicious", action plan 3 is fired instantly to protect the system. Actions that could be executed for this plan include:

- Drastic action like cutting off the node and restoration of the links. Allowing nodes in MANET to observe several types of abnormal behavior makes it possible for the nodes to route around the misbehaved nodes and isolate them or delete the path containing malicious nodes.
- Immediately close the connection (Server will not wait to receive any data). If one requires a message to be sent back to user (agent), the redirection feature should be used instead of deny feature, to redirect specific document to specific users (agent).

Thus, with the help of the intruder identification mechanism and action plans, malicious nodes that create threat to the components in the network will be removed from the network. This can be achieved by tracking the addresses of the nodes that generate abnormal values for the selected metrics. Those nodes with the specific address can then be disconnected or blocked or automatically denied future connections from accessing the network. This is achieved by means of modifying the routing protocol that controls the nodes participating in the network.

4. Mathematical Analysis

In this section, we mathematically analyze the response model and compute the mean square error, which is the summation of false positives and false negatives in identifying an intruder for a node under threat, of the response framework. False-positive represents the number of incorrectly isolated neighboring nodes for the node under threat and false-negative represents the number of not isolated neighboring nodes which should have been isolated for the node under threat.

Since 'Yes' and 'No' are the only possible outcomes in identifying the true nature of the intruder, where 'Yes' represents the correct Identification and 'No' represents the wrong Identification, the probability of correct identification of the N neighboring nodes can be obtained by applying the binomial distribution:

$$P(X=k) = C_k^N \times p^k \times (1-p)^{N-k} \quad (1)$$

Here k represents the number of nodes that are correctly estimated using the intruder identification and response framework, and can take any value from 1 to N; p represents the probability of correct identification. The Mean Square Error (MSE) is given by the sum of the variance and the square of the bias i.e.,

$$MSE = \text{variance} + \text{bias}^2 \quad (2)$$

where bias is defined as the distance between the estimator's mean and the parameter's (truth value's) mean [14]. For the binomial probability distribution, variance is given by:

$$\text{variance} = N \times p \times (1 - p) \quad (3)$$

where p is the probability of the success and N is the number of trials [14].

Proposition:

The flag M_{iz} of the intruder identification and response framework indicates if the neighboring node to the node under attack (i) is malicious or not, such that, if the mean squared error (MSE) defined by $E[(M_{iz} - \text{Truth})^2]$ is computed on each neighboring node for a node under threat (i), then the sum of the MSE on all the neighboring nodes $(\sum_{z=1}^{N} E[(M_{iz} - \text{Truth})^2])$ for a node under threat is approximately equal to $0.09N$, where N is the number of neighboring nodes. Truth is the unknown reality (i.e. the state of the neighboring node) which is to be estimated using M_{iz}.

Proof:

Let M_{iz} represents the flag of the z^{th} neighbor to the node i that is under threat. Let M_{iz} takes a value of '1' and '0' as given by the following definition.

$$M_{iz} = \begin{cases} 1 \text{ if } abnormalcounter_{iz} > normalcounter_{iz} + uncertaincounter_{iz} \\ 0; \text{ otherwise} \end{cases} \quad (4)$$

In the above equation, $abnormalcounter_{iz}$ is the abnormal counter value of the z^{th} neighbor to the node i that is under threat; $normalcounter_{iz}$ is the normal counter value of the z^{th} neighbor to the node i that is under threat, and $uncertaincounter_{iz}$ is the value of the uncertain counter of the z^{th} neighbor to the node i that is under threat.

From the experimental results obtained by simulating the intruder detection and response algorithm for DoS attacks on MANET nodes, the probability p of correctly identifying a neighboring node as an intruder node or a normal node is 0.9. Hence, applying equation 4.3, variance= $N \times 0.09$, where N is the number of neighboring nodes for the node under threat. Also based on the sample simulation data, $bias^2$ is estimated to be 0.03. Thus, applying equation 4.2, $MSE = 0.09N + 0.03$. □

5. Simulation Experiment and Results

5.1 Simulation Environment

Figure 3 shows the simulated MANET. Nodes (denoted by Ni) are connected within the mobile ad hoc network environment and mobile agents (denoted by Mi) are dispatched by a source node to a destination node for service purposes. The simulation of the MANET was carried out using NS2.

The description of the NS2 package, its input and output parameters and its use in simulation is explained with details in [12]. The parameters for the MANET to be simulated were specified using the OTcl configuration script [12]. The routing protocol used in NS2 for mobile ad hoc networks were the Ad hoc On Demand Distance Vector (AODV) and Destination Sequenced Distance Vector (DSDV) routing protocols. The network parameters considered for analysis were: packet drop rate, energy consumption and queue length based on the identification of significant parameters experiments using the classification trees methodology and training dataset. The thresholds values of the significant parameters are computed using six-sigma methodology and training dataset.

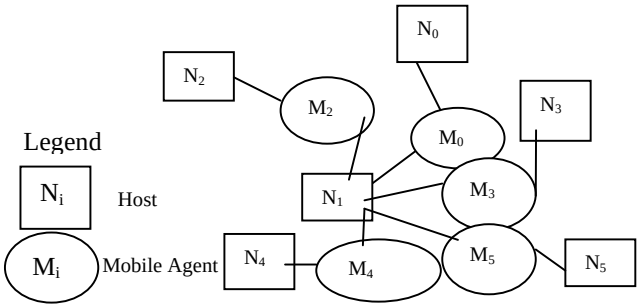

Figure 3. Simulated MANET

In order to study the feasibility and performance of the proposed MANET intruder identification and response framework, we carried out extensive simulation experiments using various MANET parameters. In our simulation, the channel type was set to wireless channel type and TwoRayGround model was used as the propagation model. The Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs was used as the MAC layer protocol. An unslotted carrier sense multiple access (CSMA) technique with collision avoidance (CSMA/CA) was used to transmit the data packets. The radio model was modeled as a shared-media radio with all nodes having the same channel capacity of 2 Mb/s and a transmission range of 250 m. In the simulation, six mobile nodes were set to move in a 1000 meter x 500 meter rectangular region. Each node was set to move independently with the same average speed. The mobility model we used was the random waypoint (RW) model. In RW model, a node randomly selects a destination from the physical terrain. It moves in the direction of the destination in a speed uniformly chosen between the minimal and the maximal speed. After it reaches its destination, the nodes stay there for a pause time and then

moves again to a newly selected destination. In our simulation, the minimal speed was 3 m/s, and the maximal speed was 15 m/s. The pause time, which affects the relative speeds of the mobile nodes, was varied. Simulations were run for 1000 simulated seconds.

Constant bit rate (CBR) traffic sources were used. The source-destination pairs were spread randomly over the network to generate CBR traffic. The size of all data packets was set to 512 bytes. The configuration used for the simulation was a Pentium-based computer with the Redhat 9.0, Linux Kernel 2.6, operating system.

5.2 Simulation Experiment

In our simulation experiments, we considered the denial of service (DoS) attack on a host node by a set of mobile agent based nodes in MANET. These attacks by mobile agent based mobile nodes cause the network to be loaded excessively, thus causing enormous retransmissions, which consumes excessive amount of host resources and hence the host cannot service genuine agents properly [2]. In this case as shown in Figure 3, the mobile agents M_0, M_2, M_3, M_4, and M_5 dispatched by host N_0, N_2, N_3, N_4, and N_5 respectively need to get serviced by N_1. However, due to DoS attack by agent M_2, the host N_1 could not service the genuine agents M_0, M_3, M_4, and M_5

The basic steps of the simulation experimentation were as follows: Agent M_2 dispatched by node N_2 was configured to send heavy traffic to Node N_1, while all other nodes received normal traffic from their agents. Node N_1 was detected to be under attack by the intrusion detection framework [2]. So its neighboring nodes N_0, N_2, N_3, N_4, and N_5 were subjected to intruder identification and response algorithm. The intruder was identified to be N_2 and it was isolated from the network by disabling its send and receive function in the routing protocol. This was implemented in NS2 by modifying the C++ code DSDV.CC in NS2. The values of the significant network parameters were observed before and after the attack and also after the response. After the response, Node N_1 was detected to be normal by the intrusion detection framework.

5.3 Experimental Results

Figures 4 through 9 give the plot of the values of the significant attack sensitive parameters without the response and with the response applied, for each neighboring node to the node under threat N_1. Figures 4 and 5 represent the control chart for the queue length metric during the DoS attack and after the response respectively. As seen in the Figure 4, queue length metric for the link between source node N_2 and host N_1 is significantly above the vulnerable state threshold (1157) when no response is applied during the attack. After the response is applied, the queue length metric for the link between node N_2 and the host N_1 is within the normal state threshold control limit as seen in Figure 5, since it is cut off from the network.

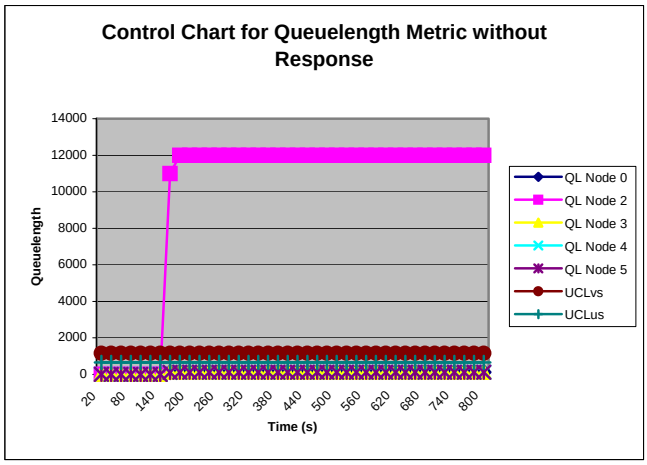

Figure 4. Queue Length Metric without Response

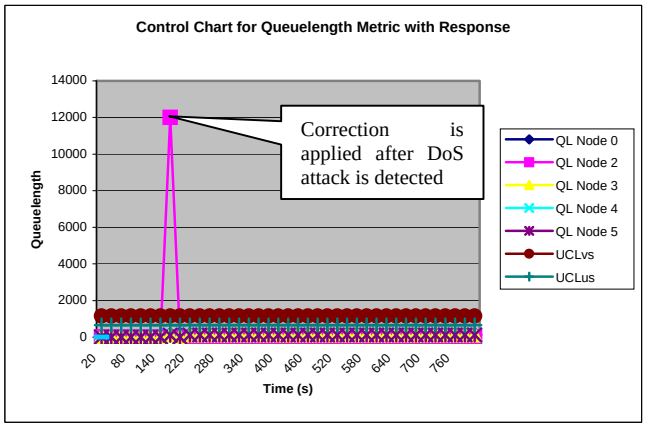

Figure 5. Queue Length Metric with Response

Figures 6 and 7 represent the control chart for PD metric during the DoS attack and after the response respectively. As shown in Figure 6, the PD for the link between source node N_2 and host is significantly above vulnerable state threshold (208) without response.

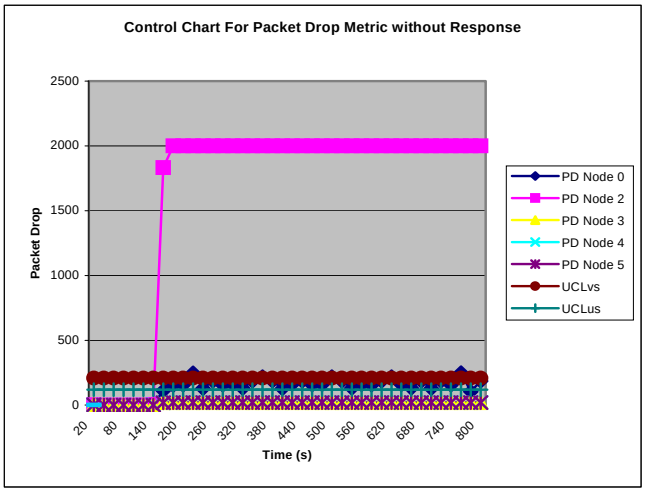

Figure 6. Packet Drop Metric without Response

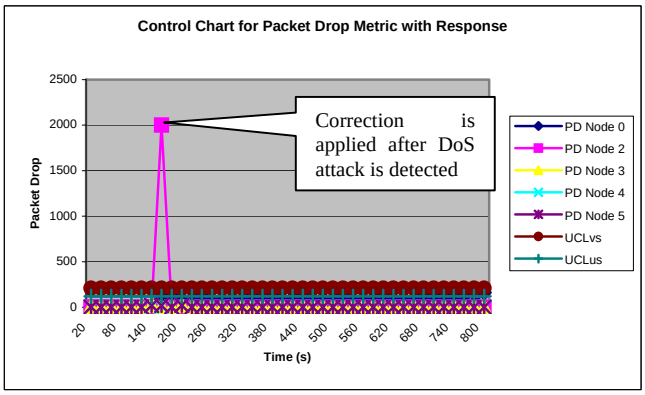

Figure 7. Packet Drop Metric with Response

As shown in Figure 7, once the malicious node N_2 is identified and isolated from the network, there are no packet drops associated with the malicious node N_2. Figures 8 and 9 represent the control chart for the energy consumption (EC) metric during the DoS attack and after the response respectively. As shown in Figure 8, the energy consumption metric for source node N_2 is significantly above the vulnerable state threshold (2 joules) when no response is applied during the attack. After response is applied, EC metric for N_2 is within normal limit.

Thus upon detecting that a node is under threat, the neighboring nodes are subjected to the response and protection mechanism, which identifies the intruder and isolates it. This protects the node under threat and hence the entire network. Similar results were obtained when both AODV and DSDV were used as the routing protocols.

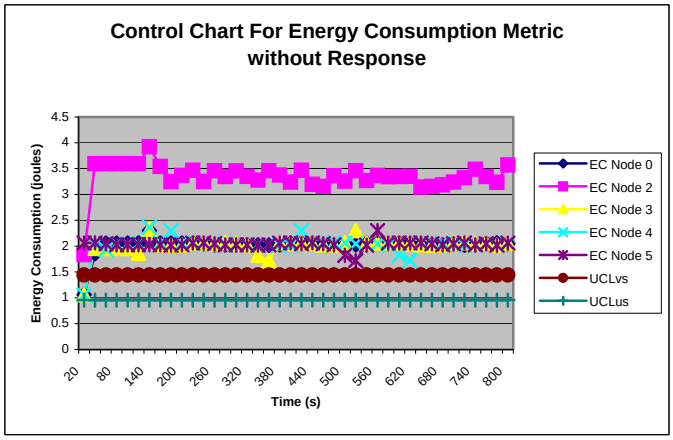

Figure 8. Energy consumption metric without response

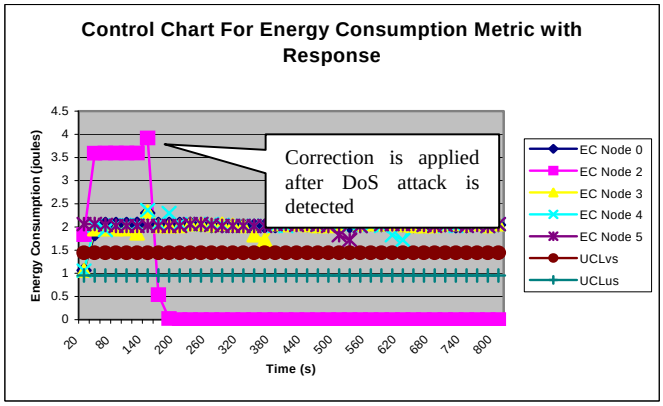

Figure 9. Energy consumption metric with response

6. Conclusion

In this paper, we have proposed an intruder identification and response framework for mobile ad hoc networks. The model is based on identifying the intruder by monitoring and measuring critical attack sensitive parameters that are affected by various types of attacks and exercising response action plans to counter the attack and protect the MANET from the intruder. Experimental results of the model simulated using NS2 with AODV and DSDV as the MANET routing protocol for Denial of Service attack demonstrate the validity of our intruder identification and response framework.

References

[1] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in Proceedings of the MobiHoc Conference, 2001, pp. 146-155.

[2] S. P. Alampalayam and A. Kumar, "Adaptive security model for mobile agents in wireless networks," in Proceedings of IEEE GlobeCom Conference, 2003, pp. 1516-1521.

[3] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," Wireless Networks, vol. 9 no. 5, pp. 545-556, Sep 2003.

[4] G. Vigna, S. Gwalani, K. Srinivasan, E. Belding-Royer, and R. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," in Proceedings of 20thACSA Conference, 2004, pp. 16-27.

[5] R. Puttini, J. Percher, L. Me, and R. Sousa, "A fully distributed IDS for MANET," in Proceedings of IEEE Symposium on Computers and Communications, 2004, pp. 331-338.

[6] S. P. Alampalayam, A. Kumar, and S. Srinivasan, "Mobile ad hoc networks security – a taxonomy," in Proceedings of ICACT Conference, 2005, pp. 839-844.

[7] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C. Y. Tseng, T.Bowen, K. Levitt, and J. Rowe, "A general cooperative intrusion detection architecture for MANETs," in Proceedings of the 3rd IEEE International Workshop on Information Assurance, 2005, pp. 57-70.

[8] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proceedings of the 3rd International Conference on Pervasive Computing and Communications, 2005, pp. 191-199.

[9] R. Puttini, J. Percher, L. Me, O. Camp, and R. De Souza, "A modular architecture for distributed IDS in MANET structures," Lecture Notes on Computer Science vol. 2669, pp.91-113, Springer-Verlag, May 2003.

[10] S. Bhargava and D. P. Agrawal, "Security enhancements in AODV protocol for wireless ad hoc networks," in Proceedings of IEEE Vehicular Technology Conference, 2001, pp. 2143-2147.

[11] D. Karig and R. Lee, "Remote denial of service attacks and countermeasures," Princeton University, Department of Electrical Engineering Technical Report CE-L2001-002, 2001.

[12] NS2 [online] available: www.isi.edu/nsnam/ns accessed Jan. 2009.

[13] N. Stakhanova, S. Basu, and J. Wong, "Taxonomy of intrusion response systems," Computer Science, Iowa State University, Technical Report 06-05, 2006.

[14] Agresti and Franklin, Statistics: The Art and Science of Learning from Data. NJ:Prentice Hall, 2006.

[15] S. P. Alampalayam and A. Kumar, "Predictive security model using data mining," in Proceedings of IEEE GlobeCom Conference, 2004, pp. 2208-2212.

[16] S. P. Alampalayam and A. Kumar, "An adaptive and predictive security model for mobile ad hoc networks," Kluwer Personal Communications Journal, Security Special Issue for Next Generation Wireless Networks, vol. 29, pp. 263-281, June 2004.

[17] Yingfang Fu, Jingsha He, Guorui Li, "A Distributed Intrusion Detection Scheme for Mobile Ad Hoc Networks", in Proceedings of Computer Software and Applications Conference, 2007. COMPSAC 2007, pp. 75-80.

[18] N.Komninos, D.Vergados, C.Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks", Ad Hoc Networks 5(3), 2007, pp. 289-298.

[19] Mitrokotsa, M. Tsagkaris, C. Douligeris, "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms", In Proceedings of the seventh Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2008)

[20] A. Mitrokotsa, N. Komninos, C. Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET", In Proceedings of IEEE International Conference on Pervasive Services 2007, pp. 118 – 127.

[21] A. Mitrokotsa, N. Komninos, C. Douligeris, "Towards an Effective Intrusion Response Engine Combined with Intrusion Detection in Ad Hoc Networks", In Proceedings of the Sixth Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007).

[22] A. Mitrokotsa, N. Komninos, C. Douligeris, "Intrusion Detection and Response in Ad hoc Networks",Advances in Ad Hoc Network Security, International Journal on Computer Research, Nova Science Publishing Inc., Volume 15, Issue 1, 2007

Biographies of the Authors

Dr. Sathish Alampalayam Kumar (Sathish) obtained his PhD in computer science and engineering from Uni-versity of Louisville, Kentucky, US in 2007. He also completed his MBA from University of Louisville, Kentucky, US in 2001. Currently, he is working as IT Solution Delivery Manager in US and as an Adjunct Faculty at the Department of Computer Science, California State University, Los Angeles, California, US.

Sathish has more than 15 years of industry, teaching and research experiences in US. Also, he has more than 10 publications in refereed journals and conferences at the international level. His current research contributions are in the areas of mobile ad-hoc networks, in particular, the security architectures and algorithms for this type of networking. He was also listed in Marquis Who's Who in Science and Engineering 2007, Who's Who in World 2008 and Who's Who in America 2009.

Dr. S. Srinivasan (nickname Srini) is a Professor of Computer Information Systems and Director, Information Assurance Group at the University of Louisville. He joined U of L in 1987. His research interests are in Information Security. He has published several papers in both Mathematics and Computer Science.He is heading the InfoSec program development at the University of Louisville, which was designated a National Center of Academic Excellence by the National Security Agency and the Department of Homeland Security. Also, he is leading U of L's Gifted Student Summer Program, which attracts bright students to a three-week summer academic program at U of L. This program has attracted students from all parts of Kentucky and other states. Currently he concentrates his teaching in Information Security and Databases. He volunteers his time extensively for public education causes.