Intruder Identification and Response Framework for Mobile Ad hoc Networks

S. P. Alampalayam\textsuperscript{1}, Anup Kumar\textsuperscript{1}, J. H. Graham\textsuperscript{1}, S. Srinivasan\textsuperscript{2}  
\textsuperscript{1}Computer Engineering and Computer Science Department  
\textsuperscript{2}Computer Information Systems Department  
University of Louisville, Louisville, KY 40292, USA  
\{spalam01, ak, jhgrah01, srini\}@louisville.edu

ABSTRACT

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, we have proposed an intruder identification and response framework for MANET. Experimental results of the model simulated in NS2 for selected denial of service (DOS) attacks are very promising.

Keywords: 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 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. 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 [1]. 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]. 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 an intrusion response approach (IRA).

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. Section 5 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 6 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., 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 [9]. Bhargava et al., have proposed a security model for AODV routing protocol to prevent intrusion attacks in MANET [10].

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. 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.

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. MANET INTRUDER IDENTIFICATION AND RESPONSE FRAMEWORK

This section explains the proposed intruder identification and response framework for MANET. 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, the response framework examines each neighboring source node to the node under threat, and different action plans are initiated based on the identification of the nature of the neighboring nodes.

3.1 Architecture

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.

![Figure 1 Architecture of the intruder identification and response framework](image-url)
Based on the reputation counter that is evaluated, the reputation flag is asserted as “Normal”, “Uncertain” or “Malicious”. If the reputation flag is “Normal”, no action is necessary. If the reputation flag is “Uncertain” or “Malicious”, response action plans are executed to protect the MANET. The response action plans isolate, disconnect, block or automatically deny future connections to malicious nodes.

Figure 1 shows a time period check logic between “No action required” block and “monitor significant parameters” block. If there is no time period check between “No action required” block and “monitor significant parameters” block, the response framework would create an unnecessary overhead. This is due to the reason that continuous monitoring is expensive in terms of resources needed. Hence, a timed periodic check is applied in the framework.

Thus, this framework is based on monitoring the network parameters and performing response action plan on the basis of assertion of reputation flag. Such a framework allows for response to selfish and malicious node attacks. Those malicious and selfish nodes with a specific IP address that generate abnormal metric parameter values are identified and gradually isolated.

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 sum of normal and abnormal counters, “uncertain” flag is asserted. If the value of the abnormal counter is greater than sum of normal and uncertain counters, “malicious” 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. INTRUDER IDENTIFICATION ALGORITHM
Intruder Identification algorithm is shown in Figure 2.

1. Let \( N_1, N_2, ..., N_k \) be the nodes which are detected to be under threat based on Intrusion Detection Algorithm.
2. Let \( x_1, x_2, ..., x_n \) be the significant metric parameters.
3. For each node under threat \( (N_i) \), where \( 1 \leq i \leq k \) and ‘k’ being the number of nodes under threat

3.1. For each adjacent source node, \((M_j)\), where \( 1 \leq j \leq n \) and ‘n’ being the number of adjacent source nodes to the node under threat

3.1.1 Initialize its \{abnormal, uncertain, normal\}counter

3.1.2 For each significant parameter \((x_j)\), where \( 1 \leq j \leq n \) and ‘n’ being the number of significant parameters
- Identify the parameter value \((Val(x_j))\) for the node \(M_j\).
- If \(Val(x_j)\) is in \{abnormal state, uncertain state, normal state\} increment the \{abnormal, uncertain, normal\}counter of source node \((M_i)\) respectively.
- Abnormal state can have very high values or very low values depending on the nature of the parameter.

3.2. For each adjacent source node \((M_i)\)

3.2.1 if \((\text{its abnormalcounter}_i \text{ is greater than sum of normalcounter}_i \text{ and uncertaincounter}_i)\)
- \{set the flag for node \((M_i)\) to malicious\}
else
- if \((\text{its uncertaincounter}_i \text{ is greater than sum of abnormalcounter}_i \text{ and normalcounter}_i)\)
- \{set the flag for node \((M_i)\) to uncertain\}
else
- \{set the flag for node \((M_i)\) to normal\}
end-if

3.2.2 if \((\text{flag of node } M_i \text{ is malicious})\)
- \{Execute Action Plan 3: this plan executes drastic action like cutting off the node and restoration of the links.\}
else if \((\text{flag of node } M_i \text{ is uncertain})\)
- \{Execute Action Plan 2: this plan executes moderate response action like automatic re-authentication of the node.\}
else
- \{Execute Action Plan 1: No action is needed since the node is neither malicious nor selfish. In order to avoid unnecessary overhead, apply time period check before further collaborative monitoring, whenever the action plan is Action Plan 1\}
end-if

Figure 2. Intruder Identification Algorithm

5. SIMULATION EXPERIMENT AND RESULTS
5.1 Simulation Environment
Figure 3 shows the simulated MANET. Nodes (denoted by \( N_i \)) are connected within the mobile ad hoc network environment and mobile agents (denoted by \( M_i \)) 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 was the Ad hoc On Demand Distance Vector (AODV) routing protocol. 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.

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 M₀, M₂, M₃, M₄, and M₅ dispatched by host N₀, N₂, N₃, N₄, and N₅ respectively need to get serviced by N₁. However, due to DoS attack by agent M₂, the host N₁ could not service the genuine agents M₀, M₃, M₄, and M₅.

The basic steps of the simulation experimentation were as follows: Agent M₂ dispatched by node N₂ was configured to send heavy traffic to Node N₁, while all other nodes received normal traffic from their agents. Node N₁ was detected to be under attack by the intrusion detection framework [2]. So its neighboring nodes N₀, N₂, N₃, N₄, and N₅ were subjected to intruder identification and response algorithm. The intruder was identified to be N₂ 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 N₁ 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 N₁. 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 N₂ and host N₁ 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 N₂ and the host N₁ is within the normal state threshold control limit as seen in Figure 5, since it is cut off from the network.
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.

Figure 8. Energy consumption metric without response

Figure 9. Energy consumption metric with response

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.

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 as the MANET routing protocol for Denial of Service attack demonstrate the validity of our intruder identification and response framework.

ACKNOWLEDGEMENTS
This work was funded in part by grants from the Treasury Dept. and the National Science foundation. The opinions and conclusions reported here are those of the authors.

REFERENCES