www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10743-10749

Improving Network Performance Using An Intrusion Detection & Adaptive Response Approach For Manets

Karthigha M, Rangarajan Gowtham S
Assistant Professor, Department of CSE(PG)
Sri Ramakrishna Engineering College,
Coimbatore.
PG Scholar, Department of CSE(PG),
Sri Ramakrishna Engineering College,
Coimbatore.

***Abstract*— A mobile ad hoc network (MANET) is normally a, infrastructure-less network of mobile devices connected without wires. But protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs). Mobile ad hoc networks are vulnerable to a variety of network layer attacks such as black hole, gray hole, sleep deprivation & rushing attacks. Intrusion detection and prevention provides a way to protect mobile ad hoc networks (MANETs) from attacks by external or internal intruders. So, in the existing system cost sensitive model for Intrusion Response Systems (IRS) is used in fixed networks. This technique relies on comparing the cost of deploying a response against the cost of damage caused by an "un-attended" intrusion and decides to preemptively deploy a response with maximum benefit. But the problem is In MANETs it is difficult to calculate the intrusion response cost, which we can define as the negative impact on the network resources caused by the response. So, in the proposed system an intrusion detection & adaptive response mechanism (IDAR) for MANETs is presented that detects a range of attacks and provides an effective response with low network degradation. The deficiencies of a fixed response to an intrusion are considered and we overcome these deficiencies with a flexible response scheme that depends on the measured confidence in the attack, the severity of attack and the degradation in network performance. We present results from an implementation of the response scheme that has three intrusion response actions. Simulation results show the effectiveness of the proposed detection and adaptive response mechanisms in various attack scenarios. An analysis of the impact of our proposed scheme shows that it allows a flexible approach to management of threats and demonstrates improved network performance with a low network overhead.**

Keywords— *mobile ad-hoc network and intrusion detection system*

1.INTRODUCTION

MANET stands for "Mobile Ad Hoc Network". A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

Some MANETs are restricted to a local area of wireless devices, while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

1.1 Overview Of The Project

A mobile ad hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

1.2 Types and importance of Manet

Vehicular Ad hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment. Internet based mobile ad hoc networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal adhoc routing algorithms don't apply directly. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent

manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

1.2.1 Importance of Manet

Self-configuring network of mobile routers (and associated hosts) connected by wireless links.This union forms a random topology.Routers move randomly free Topology changes rapidly and unpredictably Standalone fashion or connected to the larger Internet. Suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations, etc.

General protection approaches [12,4,1,6,8] do not consider attack responses at all, and some other proposed MANET IDSs,for example [9,2,7] respond to intrusion in a predetermined fixed way by isolating or banning the detected intruder nodes. However, in some cases authors have focused on the intrusion response and presented new ways of responding to intrusion. Agent based cooperative intrusion response was proposed in[10]. For example, a cost sensitive model for Intrusion Response Systems (IRS) in fixed networks was proposedin [13]. In MANETs it is difficult to calculate the intrusion response cost, which defines as the negative impact on the network resources caused by the response. Firstly [13] estimate a Topology Dependency Index (TDI) which indicates how much the routing service of nodes in the network will be disrupted if the intruder is isolated. Then they estimate the Attack Damage Index (ADI) that indicates the damage caused by an attack. The ADI calculates the damage in terms of the number of nodes that are affected by the attack. Finally, they respond to the intrusion by isolating the attacker if the ADI is greater than the TDI. This cost sensitive model was proposed for the proactive routing protocol OLSR where complete network topology information is available for every node. However, this approach is not suitable for reactive routing protocols such as AODV & DSR because they only provide partial topology information; for example, in AODV a node only knows its next hops towards the source or destination of active paths.

In the proposed method, an intrusion detection & adaptive response mechanism (IDAR) is presented that employs a combination of both anomaly based and knowledge based intrusion detection techniques, and takes advantage of both techniques to protect MANETs against a variety of attacks. The proposed algorithm is considered that responds to intrusion in all cases by isolating the intruding nodes in a predetermined fixed way. The impact on a MANET's performance of (a) various attacks and (b) the fixed intrusion response (isolation) is investigated of the previous algorithm. The results of this investigation enable us to identify the deficiencies of the fixed response approach. By using this method, network layer attacks such as black hole, gray hole, sleep deprivation & rushing attacks is detected.

2. PROPOSED SYSTEM

Intrusion detection and prevention provides a way to protect mobile ad hoc networks (MANETs) from attacks by external or internal intruders. In the existing method, an intrusion detection &adaptive response mechanism (IDAR) is presented that employs a combination of both anomaly based and knowledge based intrusion detection techniques, and takes advantage of both techniques to protect MANETs against a variety of attacks. The previously proposed algorithm considered that responds to intrusion in all cases by isolating the intruding nodes in a predetermined fixed way. The impact on a MANET's performance is investigated of (a) various attacks and (b) the fixed intrusion response (isolation) of the previous algorithm. The results of this investigation enable us to identify the deficiencies of the fixed response approach. To overcome these deficiencies, in this work an adaptive flexible intrusion response scheme is presented. This new scheme selects the intrusion response action based on the severity of the attack, the degradation in network performance and the expected impact of the response action on the network performance. The intrusion response scheme has a reduced impact on network performance, and works by adaptively selecting the intrusion response action based on the level of confidence in the detection of the attack, the attack severity and the degradation in network performance. The use of a decision table to represent the intrusion response action selection criteria allows a flexible approach to management of threats and can accommodate the different security requirements of the network. IDAR demonstrates the importance of a flexible response that takes account of network conditions and attack type.

2.1 Problem Objective

Security issues in MANET are very important concern for the functionality of the network. MANET has an open medium; changing its topology dynamically due to these characteristics so it can be accessible both legitimate users and malicious attackers. Mobile ad hoc networks are vulnerable to a variety of network layer attacks such as black hole, gray hole, sleep deprivation & rushing attacks. Causing packet loss due to attacks by malicious nodes is one of the most important problems in the mobile adhoc networks. The specific objective of this research is to improve the network performance in terms of packet loss, throughput, end-to-end delay and energy consumption.

2.2 Architecture Diagram

Fig1. This architectural model considers MANET nodes as routers with hosts attached, as illustrated in fig 1. These attached hosts may be "external" or "internal" – however the important observation to make is, that the links between these hosts and the router are classic IP links, behaving as described. This implies that, from the point of view of the hosts, and the applications running on these hosts, connectivity is via a classic IP link. Hosts, and their applications, are not exposed to the specific characteristics of the MANET interfaces and are connected to the MANET via a router, which has one or more MANET interfaces. Since the hosts in figure. are connected to a classic IP link, these hosts are configured and behave as hosts in any other network, and the links to which they are connected have properties identical

to those any classic ip link.

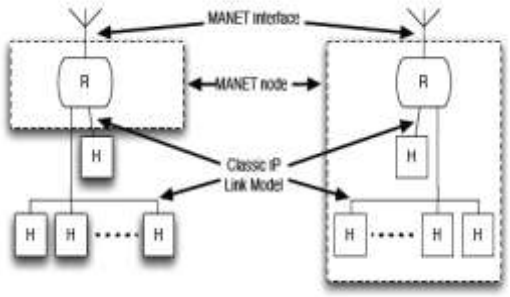

Fig 1. Architecture of Manet

2.3 Advantages

- Improving the network performance
- Overhead is less
- Detect the attacks in the mobile adhoc network
- High detection accuracy

3. RELATED WORK

1. A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks by Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar[15].

Protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs). In this work, a mechanism is presented for detection of malicious gray hole nodes in MANETs. Due to their occasional misbehavior, the gray holes are very difficult to detect.

In this work, a security mechanism is proposed to defend against a cooperative gray hole attack on the well known AODV routing protocol in MANETs. A gray hole is a node that selectively drops and forwards data packets after it advertises itself as having the shortest path to the destination node in response to a route request message from a source node. The proposed mechanism does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to malicious activities of any node. This security mechanism increases the reliability of detection by proactively invoking a collaborative and distributed algorithm involving the neighbor nodes of a malicious gray hole node. Detection decision works on a consensus algorithm based on threshold cryptography. The simulation results show that the mechanism is effective and efficient with high detection rate and very low false positive rate and control overhead.

8.Structural Results for Combined Continuous UserAuthentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks by Shengrong Bu, F. Richard Yu, Xiaoping P. Liu and Helen Tang.[1]

Continuous user authentication is an important prevention-based approach to protect high security mobile adhoc networks (MANETs). On the other hand, intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities. In this work, a fully distributed scheme of combining continuous authentication and intrusion detection is presented for high security MANETs. A user authentication (or IDS) can be scheduled in a distributed manner considering both the security situations and resources (e.g., node energy) in MANETs. The distributed continuous user authentication and intrusion detection scheduling problem is formulated as a POMDP multi-armed bandit problem. The structural results method is presented for solving the scheduling problem in a large network with a variety of nodes. To show that, under reasonable conditions on MANETs, structural results can be derived for the combined continuous user authentication and intrusion detection problem, which are trivial to implement and make the solution practically useful.

4.IMPLEMENTATION

4.1 Creation of Network module

An undirected graph G (V, E) where the set of vertices V represent the mobile nodes in the network and E represents set of edges in the graph which represents the physical or logical links between the mobile nodes. Two nodes that can communicate directly with each other are connected by an edge in the graph. Let N denote a network of m mobile nodes, $N_1, N_2, .. N_m$ and let D denote a collection of n data items $d_1, d_2, .. d_n$ distributed in the network. For each pair of mobile nodes N_i andN_j, let t_{ij} denote the delay of transmitting a data item of unit-size between these two nodes. In this MANET organization, all network nodes operate in one of the three roles of manager node (MN), cluster heads (CH) and cluster nodes (CNs). Further assume a security mechanism to protect communication between MN, CHs and CNs.

4.2 Monitoring the network and data gathering

In this module, monitors the network and periodically collects data for intrusion detection and prevention throughout the network's lifetime. In the data collection phase, after each time interval (TI) the CHs gather data from the CNs within their virtual cluster. The data is stored in the form of two matrices: the network characteristic matrix (NCM) and a performance matrix (PM). The CHs then report these matrices to the MN. The NCM records data that is specific to the network routing protocol. However, IDAR is general, and different NCM parameters can be used for different routing protocols. The IDAR is illustrated using AODV as the routing protocol, and the NCM consists of the following seven parameters:

NCM= {RREP (route reply), RREQ (route request), RERR (route error), TTL (time to live) values, RREQ src_ seq, RREP dest _seq, RREQ dest _seq}

The performance matrix consists of parameters which reflect the network performance and which can be derived from NCM parameters. Here, the PM consists of the following four parameters:

PM = {RPO (routing protocol overhead), PDR (data packet delivery ratio), CPD (number of control packets dropped), Throughput}.

NCM is a two dimensional matrix of (r*c) and the number of rows (r) and number of columns (c) depend on its parameters; therefore its storage structure is dynamically assigned by the intrusion detection & adaptive response mechanism (IDAR) monitor.

4.3 Training phase

In the training phase, CHs continuously gather NCM and PM information, and at fixed time intervals report their collected data to the MN. The MN applies the training module for N for these time intervals. The NCM consists of j parameters, where j = 1 to 7 in the case study in this work. ${}_jX_k^i = X_1, X_2, X_3$ is a set of random variables representing the jth NCM parameter in the ith time interval and k = (1 to

M) represents the number of random variables in the jth NCM parameter, where M is the maximum value of the random variables of the NCM's jth parameter in the ith time interval. Similarly, the performance matrix is represented by ${}_jY_k^i$ where j = 1–4 in this work's case study. The MN calculates the probability distribution of $P({}_jX_k^i)$ for time interval i, and also calculates the PM parameters for the ith time interval. This whole process is repeated for the N time intervals. The MN then calculates the mean NCM of $P({}_jX_k^i)$ and the mean PM for N intervals, and these are stored as an initial training profile (ITP) of the NCM and PM. These initial training profiles reflect the normal behaviour of the nodes in the network and the expected network performance.

4.4 Testing phase

4.4.1 Detection of intrusion

In the intrusion detection phase the MN considers the network characteristic parameters from the NCM, and uses ABID to identify any intrusion in the network. The ABID uses the chi-square test, because it has a low computational cost and is based on distance measure, as compared to other tests such as Hotelling's T^2. The algorithm first calculates the probability distribution of each NCM parameter, and stores these as observed values. For each time interval (TI) the MN performs hypothesis testing with null hypothesis Ho[j](observed distribution of NCM fits the expected) for each parameter j of the NCM at calculated chi-computed values obtained from Eq. (1), where j is the NCM parameter and k(= 1 to M) is the number of random variables in each parameter. The MN then performs combined hypothesis testing of all parameters of the NCM.

$$\chi^2[j] = \forall_j\left(\sum_{k=1}^{M}\left(\frac{({}_jX_k^i - {}_jx_k^i)^2}{{}_j\hat{x}_k^i}\right)\right) \quad \text{.....(1)}$$

If the combined null hypothesis Ho (observed distribution of all NCM parameters fits the expected) is rejected then it assumes intrusion has occurred during the TI, and proceeds to the next stage i.e. attack identification. Else, update the initial training profile of the NCM through an exponentially weighted moving average (EWMA):

$$\forall_j\left(= {}_j\widehat{X^i_{(q,k_1^M)}} = \beta * {}_jX^i_{(q,k_1^M)} + (1-\beta) * {}_j\widehat{X^i_{(q,k_1^M)}}\right) \quad \text{.....(2)}$$

Where ${}_j\widehat{X^i_{(q,k_1^M)}}$ and ${}_jX^i_{(q,k_1^M)}$ represent the expected and observed values ofNCMparameter j for update period number q respectively. The value of q is incremented in the TI when no intrusion in the MANET is detected. k represents the random variable from 1 to M in each NCM parameter and $\beta = \frac{2}{(q-1)}$ is the weighting factor. The updated expected profile model therefore reflects the current behavior of the network.

4.4.2 Identification of attacks

If network intrusion is detected, the MN proceeds to the second stage, namely attack identification. This uses a rule-based approach to identify the attack that is taking place. IDAR maintains a knowledge base (KB) that is used in all stages of the testing phase. The knowledge base consists of facts, rules and an inference engine. A set of rules is constructed for attack and intruder identification by analyzing the existing literature of known attacks, for example [3,5,11,14] and through investigating various attacks including their impact on network performance. The KB inference engine employs forward chaining on the set of rules and looks for the goal condition fulfillment that indicates a known attack.

4.4.3 Identification of intruder

Once an attack has been identified, the MN initiates intruder identification. In this phase, the MN applies intruder identification rules that are specific to the known attack. For example in case of a black hole attack it analyzes the RREP messages received from all the nodes during the latest TI and finds the node that has initiated the false RREP packet with the highest destination sequence number. Following intruder identification, an IDS should ideally respond to the intrusion. In the original work employed a fixed intrusion response, in which the intruding node was in all cases isolated. However, as shall see, this has deficiencies and therefore, to improve the overall effectiveness of the protection mechanism introduced an adaptive flexible intrusion response scheme, described in the next section.

4.4.4 Adaptive intrusion response mechanism

We now present the new adaptive flexible intrusion response scheme. We first describe the response model's internal architecture. We then illustrate a set of possible intrusion response actions suitable for MANETs, three ofwhich are used in the case study described in Section 4.We also present the technical details of the adaptive intrusion response scheme. Finally, we give a time complexity analysis of this proposed scheme.

5.1 Intrusion response action

Most of the IDSs in the literature respond to an intrusion in a predetermined fixed manner without considering the negative impact of the response or the side effects of the IRA on the network. To enhance the effectiveness of the intrusion response and to reduce its adverse effects on the network, we first consider possible IRAs (i.e. a rangeof punishments suitable for the intruding node) that are appropriate for MANETs.

5.2 List of intrusion response actions

An example list of possible IRAs based on the various operations each network node performs on data and routing packets is as follows:

5.2.1 Isolation.

In this response action all nodes in the network punish the intruding node by completely isolating it from the network immediately, that is, simply treat theintruder as non-existent. To employ this IRA, nodes impose the following restriction in terms of data forwarding and routing service.

- Network nodes do not forward any data packets originating

from or destined to the intruding node.

- Network nodes do not route any data packets through the intruder.
- Network nodes do not send any routing packets to or through the intruder.
- Network nodes ignore all routing packets originating from the intruding node.

5.2.2 Probabilistic isolation.

In this IRA, nodes do not isolate the intruder completely; instead they apply some restriction in terms of

forwarding its data. Specifically, nodes perform the following actions:

- Network nodes only forward some of the intruding node's data packets, with a specified probability.
- Network nodes do not send any routing packets through the intruder.

This ensures the intruder is not able to initiate further routing attacks, but is still able to forward data packets for other nodes in the network.

5.2.3 Route around attacker.

In this IRA, nodes route data packets around the intruding node to stop further attacks from the intruding node while still allowing the intruder to forward data packets for other nodes. To employ this intrusion response nodes perform the following actions:

Allow the intruder to forward data packets for other nodes in the network for existing routes. Nodes process these data packets so that they will reach their destinations.

- Do not include the intruder in new route discoveries, i.e.

route the packets around the intruding node.

- Ignore all routing packets generated and forwarded by intruder (i.e. to prevent further attacks).

5.2.4 Service denial.

In this response, network nodes deny services provided to or offered by the intruder while using the intruder as an intermediate router. For this intrusion response nodes perform the following tasks:

- Network nodes do not forward any data packets originating from or destined to the intruding node.
- Network nodes ignore any further services the intruderprovides to other nodes in the network, for exampleproviding internet access.

5.2.5. No punishment.

In some cases when the attack is not severe, i.e. the performance of the network is not significantly affected, it is possible that implementingany intrusion response will cause a worse degradation of the network performance than simply ignoring the attack In these cases, the attack is simply ignored.

5.2.6. Relocation.

Another response action is to physically move a node so that it is closer to the intruder node before isolating the intruder. This approach requires the availability of network topology information to find critical nodes in the network, and also requires the network to be able to command its nodes to move as required. For example, if isolating the intruder causes network partitioning due to its location in the network then a different node can be relocated close to the intruder node first to maintain the network connectivity, and then the intruder can be isolated from the network.

5.2.7 Proposed intrusion response actions.

We consider the appropriateness of each response action in the above list of possible IRAs in terms of their side effects or any adverse impact they might have on network performance. In addition, we further analyze the appropriateness of these response actions in terms of their practical effectiveness in combating attack, mitigating damage cause by attack and stopping further attacks from the intruding node. We then propose three IRAs for our response scheme and case study based on confidence on detected attacks and the impact of the attacks on network performance. This selected set of IRAs is as follows:

5.2.8 Isolation.

This response action is used when the confidence in a detected attack is high, and the attack is severe, and the network performance has degraded considerably since the attack was launched. By isolating the intruder, nodes in the network will treat the intruder as non-existent. Although this will cause a rerouting overhead it still improves the overall network performance significantly.

5.2.9. Route around attacker.

When the confidence in the detected attack is reasonably high and the NPD is noticeable then the response scheme will employ Route Around Attacker. This stops further attacks from the intruder while still maintaining the data forwarding service in the network.

5.2.10. No punishment.

When the COA is not high or the attack is not severe and NPD is tolerable then our response scheme will simply ignore the attack. This avoids reasonable adverse effects on the network performance.

5.2.11.Technical details.

The functional of each process involved in the adaptive flexible intrusion response scheme is analyzed. To observe that given the probabilistic nature of intrusion detection an intrusion response based on a single detection of an intruding node is not sufficient. Consequently, to optimize the probability of identifying intruders correctly (i.e. with a low level of false positives), the MN maintains a test sliding window (TSW). IDAR will therefore respond to the intrusion only when the intruding node has been identified in a number of time intervals (TIs). Specifically, an intrusion response only occurs if a given intruder node is identified in at least d detections out of p TIs of the TSW. To select the appropriate values of p (representing the size of the TSW in units of TIs, i.e. the number of checks considered) and d (the minimum number of detections required to confirm a detected node as an attacker), note that the detection of an intruding node within a TSW is a Bernoulli trial (i.e. the trials during the TSW are identical and independent repetitions of the experiment with two possible outcomes: detection or no detection). The probability of confirmation of intrusion in a sequence of Bernoulli trials is therefore given by,

$$P_c = \sum_{i=d}^{p} C_i^p * (P)^i * (1-p)^{(p-i)} \quad \ldots\ldots\ldots (3)$$

The MN runs the adaptive intrusion response scheme for all nodes that have been identified as intruders in the current test sliding window. The MN first estimates the confidence on attack detected (COA) value,based on the detection and accusation information:

$$COA = w_1 * C.1 + w_2 * P_c \ldots\ldots\ldots\ldots (4)$$

In Eq. (4), Wi represents a weighting factor, where the sum of these weights equals one. CI represents the confidence interval of the chi-square test during the intrusion detection phase and Pc is the probability of confirmation. Eq. (3) returns a confidence value for Pc between 0 and 1. The MN then evaluates the NPD value using Eq. (5). This is a weighted sum of the changes in the performance matrix parameter values (i.e. throughput, packet delivery ratio, routing protocol overhead and routing packets dropped) from when there was no attack in the network to their current values, as follows:

$$NPD = w_1 * \Delta Throughput + w_2 * \Delta PDR + * \Delta RPO + w_4 * \Delta RPD \ldots\ldots (5)$$

where M represents the percentage change in the parameter between the average value in the current test sliding window and the average value of the parameter when there was no attack in the network. Once the COA and NPD values have been calculated, the MN assigns confidence levels to the COA and NPD. For the NPD again use four levels, but the precise mapping of NPD value to NPD level varies as will be seen. These levels are then used in the decision table, (from the knowledge base constructed by the network administrator) to select the intrusion response.Modeling the intrusion response selection through decision table allows the network administrator to configure and modify the intrusion response selection process for different network environments.

6. Performance Evaluation

In this section, the performance of the existing and the proposed system is compared. In the existing system, cost sensitive model is used for intrusion response systems. In the proposed system, an intrusion detection & adaptive response mechanism is used. When compared to the existing method, there is high network performance and less overhead.

6.1 AODV Overhead

The impact of IRA on the AODV overhead when (a) there is no response to intrusion, (b) fixed response and (c) adaptive intrusion response, in the cases of BH, SD, and rushing attacks. The AODV overhead comprises all control packets i.e. RREQ, RREP and RERR packets generated in the network during the simulation. The graph shows that as a result of employing the proposed intrusion response scheme the AODV overhead decreases by 6.8% & 6.4% in the cases of sleep deprivation & rushing attacks respectively.

6.2 Network Degradation Overhead

The effectiveness of the intrusion response scheme in terms of the NPD, for 25 and 50 node networks respectively. They show the Network Performance Degradation (NPD) in various attack situations when there is no response to intrusion by IDAR, when the response is intruder isolation, and in the adaptive response case. It can be seen from the graphs that the average network degradation is minimized when IDAR is used with the adaptive flexible intrusion response scheme proposed in this work. Although IDAR minimizes the damage to network performance in all attacks, we observe that in the case of mild attacks such as rushing or some GH attacks, the adaptive response significantly reduces the network degradation.

7.Conclusion and Future Work

In the presented work, an intrusion detection & adaptive response mechanism is presented for MANETs that detects a range of attacks and provides an effective response with low network degradation. IDAR cannot only detect a number of attacks but can also adaptively respond to the detected attacks to halt the attack and/or mitigate the damage caused by the attack and prevent further attacks from the intruding nodes. The intrusion response scheme has a reduced impact on network performance, and works by adaptively selecting the intrusion response action based on the level of confidence in the detection of the attack, the attack severity and the degradation in network performance. The use of a decision table to represent the intrusion response action selection criteria allows a flexible approach to management of threats and can accommodate the different security requirements of the network. IDAR demonstrates the importance of a flexible response that takes account of network conditions and attack type.

7.1 Future Enhancement

But in the mobile adhoc network some of the network layer attacks are not considered in this method such as wormhole attack and Sybil attack. So this can be consider in future work.

8.References

[1]Bu.F, Yu.F.R, Liu.P, Tang.H,(2011),Structural results for combined continuous user authentication and intrusion detection in high security mobile ad hoc networks, IEEE Transactions on Wireless Communications 10 (9) 3064–3073.

[2]Hasswa.A,Zulkernine.M,Hassanein.H,(2005)Routeguard: an intrusion detection and response system for mobile ad hoc network, in: Proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2005), vol. 3, pp. 336–343.

[3] Hu.Y, Perrig.A, Johnson.B, Rushing Attack and Defense in Wireless Ad Hoc Networks Routing Protocols,(2003), in: Proc. 2nd ACM Workshop on Wireless Security, New York.

[4] Joseph.J, Das.A, Seet.B and Lee.B, (2008),CRADS: Integrated cross layer approach for detecting routing attacks in MANETs, in: Proc. IEEE Wireless Communication and Networking Conference (WCNC).

[5] KDD Data Set used in 3rd International Knowledge Discovery and Data Mining Tool Competition,(1999). <http://kdd.ics.uci.edu/ databases /kddcup99 /kddcup99.html>.[7] Kurosawa.S ,Jamalipour.A, (2007), Detecting blackhole attacks on AODV based mobile ad hoc networks by dynamic learning method, International Journal of Network Security 5.

[7] Liu.J , Yu.F.R, Lung.C,Tang.H, (2009) ,Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks, IEEE Transactions on Wireless Communications 8 (2) 806–815.

[8] MohamedY.A, Abdullah.A.B, (2010)Implementation of IDS with response for securing MANETs, in: Proc. IEEE International symposium in information technology (ITSim), vol. 2, pp. 660–665.

[9] Mitrokotsa.A,Dimitrakakis.C, (2013),Intrusion detection in MANET using classification algorithms: the effects of cost and model selection, Elsevier Journal of Ad Hoc Networks 11 (1) 226–237.

[10] Nadeem.A, Howarth.M, (2013) , Protection of MANETs from a range of attacks using an intrusion detection and prevention system, Telecommunications Systems Journal Springer 52 (4) 2047– 2058.

[11] Ping.Y, Futai.Z, Xianghao.J , Jianhua.L , (2007) , Multi-agent cooperative intrusion response in mobile ad hoc networks, Elsevier Journal of System Engineering and Electronics 18 (4) 785–794.

[12]Sen.J,Chandra,Harihara.S.G,Reddy.H,Balamuralidhar.P,(2007). A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Network, in: Proc. IEEE ICICI.

[13] Sanzgiri.K,Belding-Royer.B,(2002), A Secure routing protocol for ad hoc networks, in: Proc. 10th IEEE International Conference on Network Protocols (ICNP' 02).

[14] Wang.S, Tseng.C.H, Levitt.K, Bishop.M, Cost-sensitive intrusion response for mobile ad hoc networks, in: Proc. 10th International Conference on Recent Advances in Intrusion

Detection, Lecture Notes in Computer Science, Springer, 2007.
[15] Yi.P, Dai.Z, Zhang.S, Resisting flooding attack in ad hoc networks, in: Proc. IEEE International Conference on Information Technology Coding & Computing ITCC, April 2005.