Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Cluster Based Intrusion Detection System Based on MRA: Misbehaviour Report Authentication

S.Subashree, Parkavi Murphy John
Computer Science and Engineering & Anna University
India

Abstract*— Mobile Ad Hoc networks are more vulnerable to intrusions as they work in an open medium and use number of co-operative strategies for network communications. Solutions that are designed for fixed networks are not always suitable for Mobile Ad Hoc Networks (MANETs) because of their dynamic nature. To overcome these conditions, researchers have developed a number of decentralized intrusion detection approaches designed specifically for MANETs. These approaches, however focused exclusively on detecting malicious behaviour in MANET it will not be sufficient for MANETs. To obtain an acceptable level of security in MANETs, we proposes a security solutions as a combination of encryption with intrusion detection mechanisms. One method is to provide IDS running on every mobile node in a network, which runs as a local detection engine which analyses local data for anomalies . This detection mechanism identifies whether there is an intrusion in the nodes taking part in the communication. But nodes in MANET typically have limited battery power, thus it is not efficient to make each MANET node always a monitoring node. Instead, a cluster of neighbouring MANET nodes can randomly and fairly elect a monitoring node, the cluster head which performs the detection activities inside the cluster.

Keywords*— MANETs, Cluster Based Intrusion Detection System (CIDS), 'Misbehaviour Report Authentication' (MRA), Routing Overhead(RO), PDR(Packet Delivery Ratio).

1. INTRODUCTION

MANET is a collection of mobile nodes which work in a medium with dynamic network topology, co-operative algorithms and lack of centralized monitoring and management . In addition to these problems, MANET nodes always have limited battery power and bandwidth. Security fundamentals describe us to provide a layered security approach to create a secured network. The first layer of defence is generally by authentication and encryption schemes. The intrusion detection systems (IDS) form the second layer of defence. Intrusion detection is one of the important techniques which protects a network against intruders. An intrusion in a network is defined as any unauthorized activities in system or network. Our CIDS tries to detect and flag alerts on attempted intrusions into a system using our important scheme called MRA(Misbehaviour Report Authentication) which identifies selfishness in the network inspite of false Misbehaviour Report. In a fixed network IDS has performed well because it has a centralized decision making authority. MANETs do not have a central authority. Hence for IDS to perform well in a MANET environment we should provide a IDS which should be a combination of encryption and Intrusion detection system . Thus cluster based approach is adopted for IDS implementations in MANETs. To initiate MRA mode, the source node first searches its local knowledge base for any alternative route to the destination node. After adopting an alternative route we circumvent the misbehaviour reported node. When the misbehaviour report is received at destination node it compares the report with its local knowledge base to authenticate the node's behaviour. If the received report is already exist in the knowledge base, and then it is safe to conclude that this report is marked as malicious. This system will act as a prevention of attack than the response of attacks.

II. Intrusion Detection System

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. Some assumptions are made in order for intrusion detection systems to work . The first assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviours, as intrusion detection must capture and analyze system activity to determine if the system is under attack . Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyse packets from network trffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows .

A.Anomaly detection systems: The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response [1]

B.*Misuse detection systems:* The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.

C.Specification-based detection: The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined.

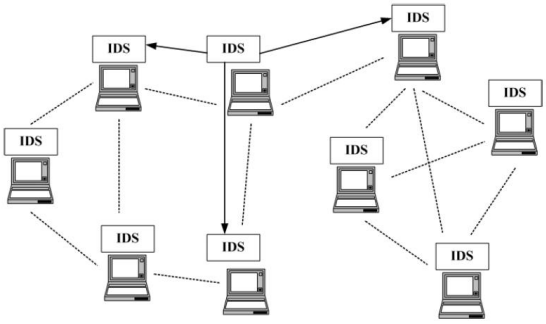

Fig.1 Intrusion detection system

III. CREDIT BASED SCHEMES

The basic idea of *credit-based* schemes is to provide incentives for nodes to faithfully perform networking functions[2]. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services.

IV. REPUTATION BASED SCHEMES

Network node collectively detect and is declare the misbehaviour of a suspicious node. Such a declaration is then propagated throughout the network, so that the misbehaving node will cut off from the rest of the network. Confident protocol proposed by Buchegger and Le Boudec is another example of reputation-based schemes. CONFIDANT consists of four important components – the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighbourhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each node continuously monitors the behaviour of its neighbours. If a suspicious event is detected, details of the event are passed to the Reputation System. Depending on how significant and how frequent the event is, the Reputation System modifies the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an *Alarm* message sent out by the Trust Manager.

V. DIGITAL SIGNATURE

Digital signatures have always been an integral part of cryptography. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity , entity authentication and data origin authentication. The security in MANETs is defined as a combination of processes, procedures and systems used to ensure confidentiality, authentication,[6] integrity and non repudiation of MANETs. It can be generalized as a data string, which associates a message with some originating entity, or an electronic analog of a written signature.

VI. PERFORMANCE METRICS

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two metrics.

A.Packet delivery ratio(PDR):

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node[3].

B.Routing Overhead(RO):

RO defines the ratio of the amount of routing-related transmissions [Route REQuest(RREQ), Route reply(RREP), Route Error(REER),ACK,S-ACK and MRA][4].

VII. PROBLEM DOMAIN

A network in this problem domain can be described as a collection of connected islands, each containing a few hundred mobile nodes and corresponding to a single routing domain. Thus providing IDS for such a network is a challenging task. Many proposed approaches to intrusion detection in MANETs rely on *promiscuous mode of monitoring* . As described by Marti, et al [6], this means that "if node A is within range of a node B, it can overhear communications to and from B even if those communications do not directly involve A." For example, suppose nodes A, B, and C are arranged in a straight line geographically such that B is within the communication ranges of both A and C, but A and C are outside

each other's range. In other words, A can communicate directly with B, and B with C, but A and C cannot, and must use B as an intermediary. Under optimal conditions, if A is promiscuously eavesdropping and B sends a packet to C, A will also overhear it. Providing intrusion detection in this manner has significant advantages. First, it allows local data collection without consumption of any additional communications overhead. Second, it provides firsthand observations (to nearby traffic); this avoids the need to rely on observations from rest of nodes, which might lie. On the other hand promiscuous monitoring can be highly unreliable under certain conditions, as described by Marti et al [6]. For example, if another neighbor of A attempts to send a packet to A at the same time B sends its packet to C, A will experience a collision and may not hear B's packet. Similarly, if node D, another neighbor of C, sends a packet to C at the same time B does, C may experience a collision. Node A may then erroneously believe that C received B's packet successfully. Therefore data from promiscuous monitoring is incomplete . The alternative to promiscuous is direct reporting by participants. For example in a network of nodes to find out which packets C received, C should explicitly report to the node. This consumes bandwidth because each packet must be retransmitted, at least once. Moreover, if C is malicious, it will not reply. bandwidth. More importantly, bandwidth consumption by reporting these values wont rise the number of packets they summarize. Thus both promiscuous monitoring and direct reporting have such pronounced advantages and disadvantages as data acquisition modes, hence our proposed CIDS is designed to support intrusion detection algorithms that use either or both.

VIII. PROPOSED WORK

A. Monitoring end to end traffic : In the network with lack of persistent traffic concentration points, network intrusion detection process must be distributed in overall of the network nodes. In our architecture, all nodes have certain responsibilities for intrusion detection tasks. The simple solution is for every node to monitor every end-to-end flow that passes through it is also monitored. An important drawback to this strategy is that it can lead to excessive redundancy and inefficient use of resources. The proposed concept of ACK is basically an end-to-end acknowledgment scheme.

1)ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet. In Ack mode, node S first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between node S and D are cooperative and node D successfully receives packet along the same route but in reverse order.within a predefined time period, if node S to node D is successful. Otherwise, node S will switch to S-ACK mode .

2)S-ACK: The S-ACK scheme is an improved version of the TWOACK scheme.The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes.For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. S-ACK mode , the three consecutive nodes work in group to detect misbehaving nodes in the network. First node N1 forwards packet to the second node then second node forwarded this to Node N3. When N3 receives packet it sends ack to N2 which in turn forwards ack to the node N1 if N1 not receives the Ack within time period it reports N2 and N3 as malicious. False Misbehaviour report is generated to node N1. Unlike TWOACK scheme our CIDS switches to MRA mode to ensure that the report is genuine or not.

B.MRA: The MRA scheme is designed to detect misbehaving nodes with the presence of false misbehaviour report generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The source node first searches its local knowledge base for any alternative route to the destination node. After adopting an alternative route we circumvent the misbehaviour reported node. When the misbehaviour report is received at destination node it compares it with its local knowledge base, If it is already received, then it is safe to conclude that this report is marked as malicious. The proposed CIDS a clustering algorithm has been proposed can run on top of any routing protocol and can also monitor the intrusions irrespective of the paths. The proposed simplified scheme has been used to detect intrusions, resulting in high detection rates and low processing and memory overhead irrespective of the paths, connections, types and mobility of nodes in the network. And implementation of the system is using NS-2 (NETWORK SIMULATOR-2) TOOL. The proposed works involves Malicious Detection Architecture and Cluster formation

C.MALICIOUS DETECTION As there is no dedicated infrastructure or central coordination, the nodes have to cooperate and self-organize to form a working communication network. A highly connected network nodes are participate and forward other node's packets. On the other hand every node has to consider its limited resources (most notably its energy). So every node is motivated to contribute as little as possible of its own energy. Usually, it is expected that all nodes forward as needed, but other policies are possible as well (e. g. only require forwarding as long as a node's battery level is high). In any way the MANET's protocols and policies imply a normative expectation on every participating node) to behave according to agreed protocols and to forward a fair amount of other node's packets as needed. As long as all nodes adhere to this and cooperate, the MANET should work without problems. One of the most important issues in designing MANET protocols is how to deal with nodes that ri not cooperate. Depending on their (or their user's) motivation I will categorize these nodes into three groups:

1)Malevolent nodes: Nodes that want to compromise the security of the MANET or of other nodes. Their actions are directed on some desired effect, but they are generally not rational because they do not strive for their own benefit maximization.

2)Selfish nodes : Nodes that do not forward other's packets ,thus maximizing their benefit at the expense of all others. They are assumed to always behave rationally, so they cheat only if it gives them an advantage.
3)Erroneous nodes : These are nodes with failing hardware or incorrect software. They do not intentionally misbehave but if they impair the working of the net, then they have to be treated just as [7] malevolent or selfish nodes.
A node is noted as malicious through checking the node against the above discussed schemes and then finally pass through MRA scheme to final as malicious one.

D.CLUSTER FORMATION: After identifying the Malicious nodes in MANETs we are just ignoring those nodes and finally forming a cluster with only trusted nodes those nodes which are reported as malicious are removed from the network . Finally formed multiple clusters with number of nodes which are trusted without any malicious that is selfish nodes. Thus our CIDS act a Prevention of attacks than the removal of attacks. Then transmission is done among the clusters only. thus we are securing the network with trusted nodes. Trusted nodes always active in communication without any delay.

Fig.2 Cluster formation

IX. ARCHITECTURE DIAGRAM

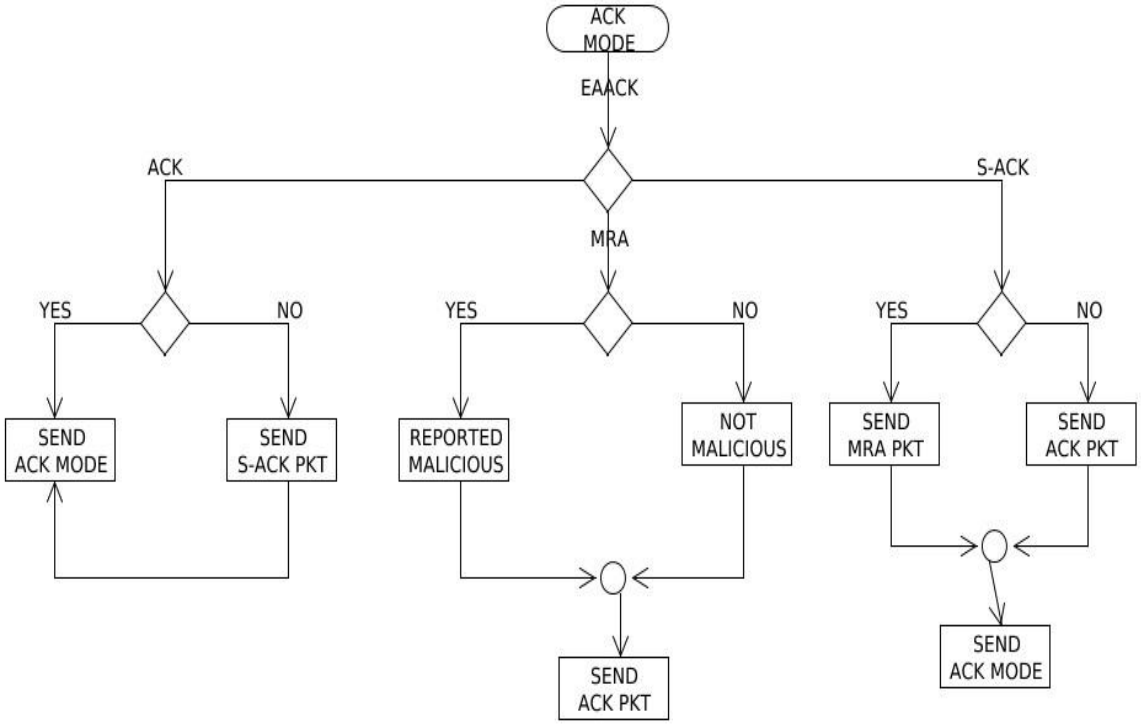

FIG.3 ARCHITECTURE DIAGRAM

X. SIMULATION RESULT

Packet delivery ratio	Malicious 0%	Malicious 10%	Malicious 20%	Malicious 30%	Malicious 40%
ACK	1	0.84	0.6	0.68	0.66
SACK	1	0.86	0.7	0.7	0.91
CIDS	1	0.96	0.98	0.92	0.92
Routing overhead	Malicious 0%	Malicious 10%	Malicious 20%	Malicious 30%	Malicious 40%
ACK	0.015	0.025	0.023	0.022	0.023
SACK	0.016	0.035	0.024	0.033	0.025
CIDS	0.3	0.3	0.037	0.047	0.61

XI. CONCLUSIONS

This Cluster Based Intrusion Detection System is used to detect Intrusion, identify the selfish nodes and isolate them from the rest of the network. The presence of a detection system will avoid malicious nodes from attempting intrusion in future. So the low-overhead clustering algorithm is proposed for the benefit of detecting intrusions in the presence of False Misbehavior Report by selfish nodes. In future the target is to make this IDS more effective and less time consuming. Also memory and processing overhead should be minimized. Cluster formation and division of head and member nodes should be instantaneous. It is also a major research task to make the IDS so powerful to detect any new type of attack.

REFERENCES

[1] Elhadi M.Shakshuki,Senior Member,IEEE,Nan Kang,"EAAK_ A Secure Intrusion Detection System For Manets"IEEE Transaction on Industrial Electronics" vol 6,no 3,MARCH 2013,PP 1089-1097.

[2] Anantvalee T and Wu J, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security. New York,2006 PP170-196.*

[3] Liu K , Deng J, Varshney P.K, and K. Balakrishnan,(2007) 'An acknowledgment-base approach for the detection of routing misbehavior in MANETs,'IEEE Trans. Mobile Comput., vol. 6, no. 5,pp. 536–550.

[4] Marti S, Giuli T.J, Lai K, and Baker K,(2000) 'Mitigating routing misbehaviour in mobile Ad hoc networks,' in Proc. 6th Annu.Int. Conf. MobileComputing Netw., Boston, MA, pp. 255–265.

[5] Nasser N and Chen Y ,(2007)'Enhanced intrusion detection systems for discovering malicious nodes in mobile Ad hoc network,' in Proc. IEEE Int.Conf. Commun., Glasgow, Scotland, pp. 1154–1159.

[6] Parker J, Undercoffer J, Pinkston J, and Joshi A,(2004) 'On intrusion detection and response for mobile Ad hocnetworks,'inProc. IEEE Int. Conf.Perform., Comput., Commun., pp. 747–752.

[7] Patwardhan A, Parker J, Joshi A, Iorga M, and Karygiannis T,(2005) 'Secure routing and intrusion detection in Ad hoc networks,' in Proc. 3rd Int. Conf.Pervasive Comput.Commun., pp. 191–199.

[8] A General Cooperative Intrusion Detection Architecture for MANETs D. Sterne1, P. Balasubramanyam2, D. Carman1, B. Wilson1, R. Talpade3, C. Ko1 [9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud(2009), 'Data transmission enhancement in presence ofmisbehaving nodes inMANETs,'Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282.

[10] A. Singh, M. Maheshwari, and N. Kumar(2011), 'Security and trust management in MANET,' in Communications in Computer and Information Science, vol. 147.New York: Springer-Verlag, pt. 3, pp. 384–387.

