Effectual Strategy for Intrusion Detection Systems in MANET

P. Prema
Assistant Professor,
Dept. of Computer Science Engineering,
Dhanalakshmi College of Engineering,
Chennai, India

U. Arul
Professor,
Dept. of Computer Science Engineering,
Dhanalakshmi College of Engineering,
Chennai, India

K. Nattarkannan
Professor,
Dept. of Computer Science Engineering,
Dhanalakshmi College of Engineering,
Chennai, India

Abstract

A mobile ad hoc network (MANET), also known as a wireless ad hoc network or wireless ad hoc network, is a continuously self-configuring, infrastructure-free network of mobile devices that are connected wirelessly. Due to the dynamic topology and the lack of conventional security infrastructures, MANETs are extremely vulnerable to attacks. Our design is based on a "self-adapting threshold scheme", which sets a predefined threshold for each type of attack and then adjusts the threshold based on the network data collected. This network-flexible approach combines the detection of anomalies (definition of anomaly rules) with the signature-based detection (pattern matching). If a wrong incident (a symptom of a known attack pattern) occurs, the counter is incremented for each type of attack. Our schema updates the status of this node to "suspicious" and continues to monitor the node for possible tampering, while details of failures such as sending the node ID, time of occurrence, etc. are sent to the neighboring nodes using the watchdog scheme.

Keywords: MANET, Wireless Network, Signature Based Detection, Anomaly Detection, Watchdog.

Introduction

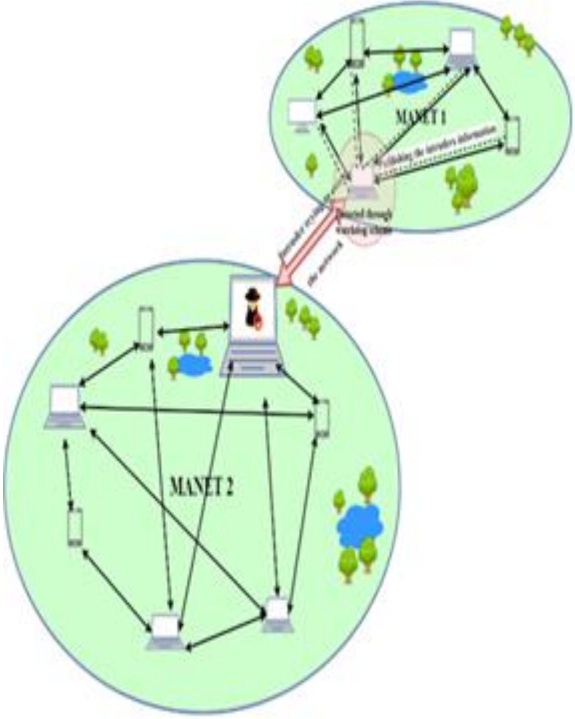
MANET stands for Mobile Ad Hoc Network. It is a kind of ad hoc network that can change locations and configure itself during operation. Since MANETs are mobile, they use wireless connections to connect to different networks. This can be a standard WiFi connection or another medium, e.g. B. a cellular or satellite transmission[1]. Some MANETs are limited to a local area of wireless devices, while others may be connected to the Internet. These networks can be set up anywhere and at any time. It is a multi-hop network with an autonomous terminal and dynamic network topology. The main areas of use for MANET are military scenarios, sensor networks, rescue operations, students on campus, conferences, etc[2]. MANET can be deployed quickly and is self-configuring. Because of the highly dynamic environment, routing in MANET is a very important task. Due to the mobile behavior of nodes, the network structure is dynamic[3]. The network is self-providing and decentralized. The nodes in MANET act both as a router and as a host and network topology that changes quickly and makes decisions in a distributed manner. Because of the dynamic behavior of the network, routing is a daring task for MANET, and the wireless connection in MANET is very prone to errors. Security, reliability, availability, scalability and service quality are some of the requirements of MANET. One of the challenges in the mobile ad hoc network is the lack of reliability between nodes due to its mobility and the rapidly changing topology. Therefore, it is more susceptible to malicious attacks. Lack of security in the network, which leads to the intruder interrupting the data transmission, which leads to data loss. To overcome these attacks and challenges in MANET intrusion detection systems, they were used in ad hoc networks[4,5]. An efficient method for detecting an attack in a MANET is the integration of an intrusion detection system (IDS). An IDS is software that simplifies the intrusion detection process. IDS's initial responsibility is to identify unwanted and intruder activity. It is the defense mechanism in the mobile ad hoc network that provides secure communication between the nodes. In contrast to the fixed infrastructure, the mobile ad hoc network lacks the access point and the routers. Because of the lack of central control, the IDS is therefore provided in every node of the ad hoc network. If an intruder is detected, it is published on other nodes in the network.

Due to its unique characteristics, MANET is being implemented more and more widely in the current circumstances. However, consider the fact that MANET is popular among the most important work applications where network security is so important. Unfortunately, remote distribution and open media MANET are vulnerable to a variety of attacks[6.7]. For example, due to the lack of physical security of the nodes, malicious attackers can easily capture and compromise the nodes to attack. Considering the fact that most routing protocols in MANETs assume that each node in the network is cooperating with other nodes and is not malicious, any attacker can easily compromise MANETs by inserting malicious nodes into the network[8,9,10].

System Architecture

System Architecture Diagram

Fig.1 System Architecture



System Architecture Description

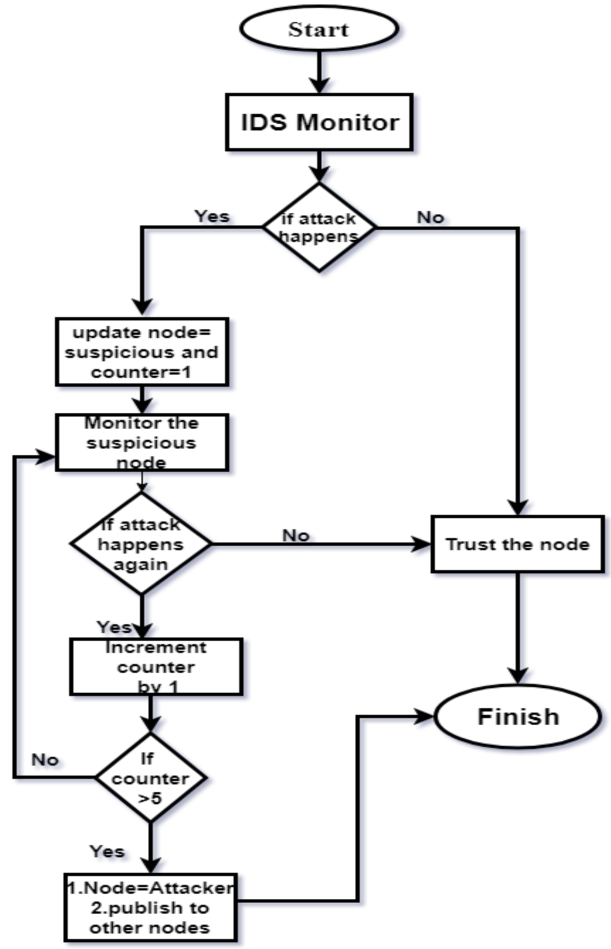
Our system architecture consists of MANETs which is a self-configuring dynamic network where each node can act as host as well as router. Each node is connected to every other nodes in the MANET.TCP connection is created between required nodes using agents such as TCP agent and sink agent[11,12,13]. An IDS in every node keeps on monitoring the network for any attack. If any of the intruder enter the network or any attack occurs on the network, the Intrusion Detection System identifies it and publish the details of the attack or intruder to every other nodes in the network through watchdog mechanism so that the nodes will neither receive packets from the intruder nor it will use it as intermediate nodes[14,15].

System Flow Logic

Descriptiom

1. Start
2. IDS monitors the network
3. If any misbehavior is detected, it updates the node as “suspicious” and set counter value as “1”, else trusts the node and go to step 6.
4. The suspicious node is then monitored for attacks.
5. If attack happens, the counter value is incremented and compared with the predefined threshold value.
6. If exceeds, the node is identified as attacker/Intruder and the details are sent to all the nodes in the corresponding network.
7. Stop

Flow chart



Proposed System

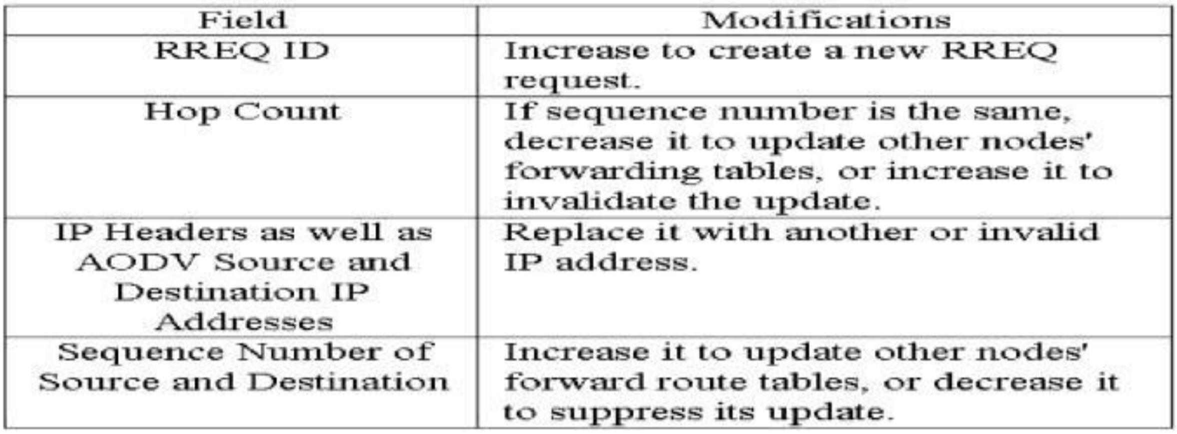
AODV, a reflection and stabilization program, builds routes if the question of whether it is an aid against different types of tasks plays a role. It is recommended that the intrusion decision be made to see if it is an AODV. The approval uses the limits to determine whether an AODV routing process can be performed and distributed to violate the term that violates the rules. It is recommended to find a certain number of people in the correct message to take the exam. In our decision we can use a very good structure and do not know what is successful to ensure that the question is answered again and again.

AODV builds rules and can be sure that Route Request (RREQ) and Route Reply (RREP) measurements are used. The first (RREQ) measurement has an RREQ ID (RID) that is best suited to find a solution for its determination. Turn around until the source appears in the routing tables and make sure that the number is updated with a message when RREQ messages are created. An answer (RREP) is only possible to ensure that the decision whether or not it is a question is the question on the subject. The following number (SN) in AODV reports that the routing data has been refreshed and other assurances that concern the frogs. The number of numbers can only be determined under two conditions: 1. When RREQ is sent from the source and 2. Determination with an RREP. The Hop Count (HC) is increased by 1 when a message (RREQ or RREP) is created for a specific help. Route Blunder Packets (RERR) will be surrounded at the beginning of routes when a connection is broken and all other nodes will leave the sections in their tables.

Identifying Fields for AODV Control Messages

The vulgar fields for AODV control fairs AODV is safe and suitable for work, but it is possible that it is not possible to make the right decision. In each AODV routing packet, some basic fields, for example, hop count, sequence numbers. F source and destination, RREQ ID, IP headers and additionally IP locations. AODV source and destination, are to fundamental redress protocol execution. Each of these flies can perform AODV functions. Table 1 shows the differences in the AODV routing messages and the effects when they are detected.

Table 1. AODV routing messages



Field	Modifications
RREQ ID	Increase to create a new RREQ request.
Hop Count	If sequence number is the same, decrease it to update other nodes' forwarding tables, or increase it to invalidate the update.
IP Headers as well as AODV Source and Destination IP Addresses	Replace it with another or invalid IP address.
Sequence Number of Source and Destination	Increase it to update other nodes' forward route tables, or decrease it to suppress its update.

Assumptions

1. We used the following supports:
2. MAC locations and IP addresses of all sorts of things are not taken into account and associated with the new secretions.
3. Network forces can get all nodes and execute all required functions.
4. There are no more drops that contain AODV messages or sticking recovery identifiers.

Figure 1. Detecting the Middle Attack

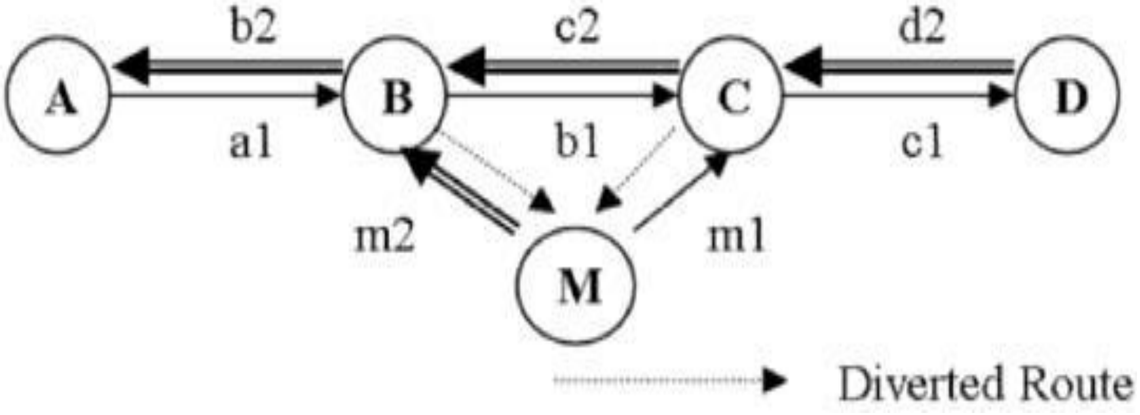
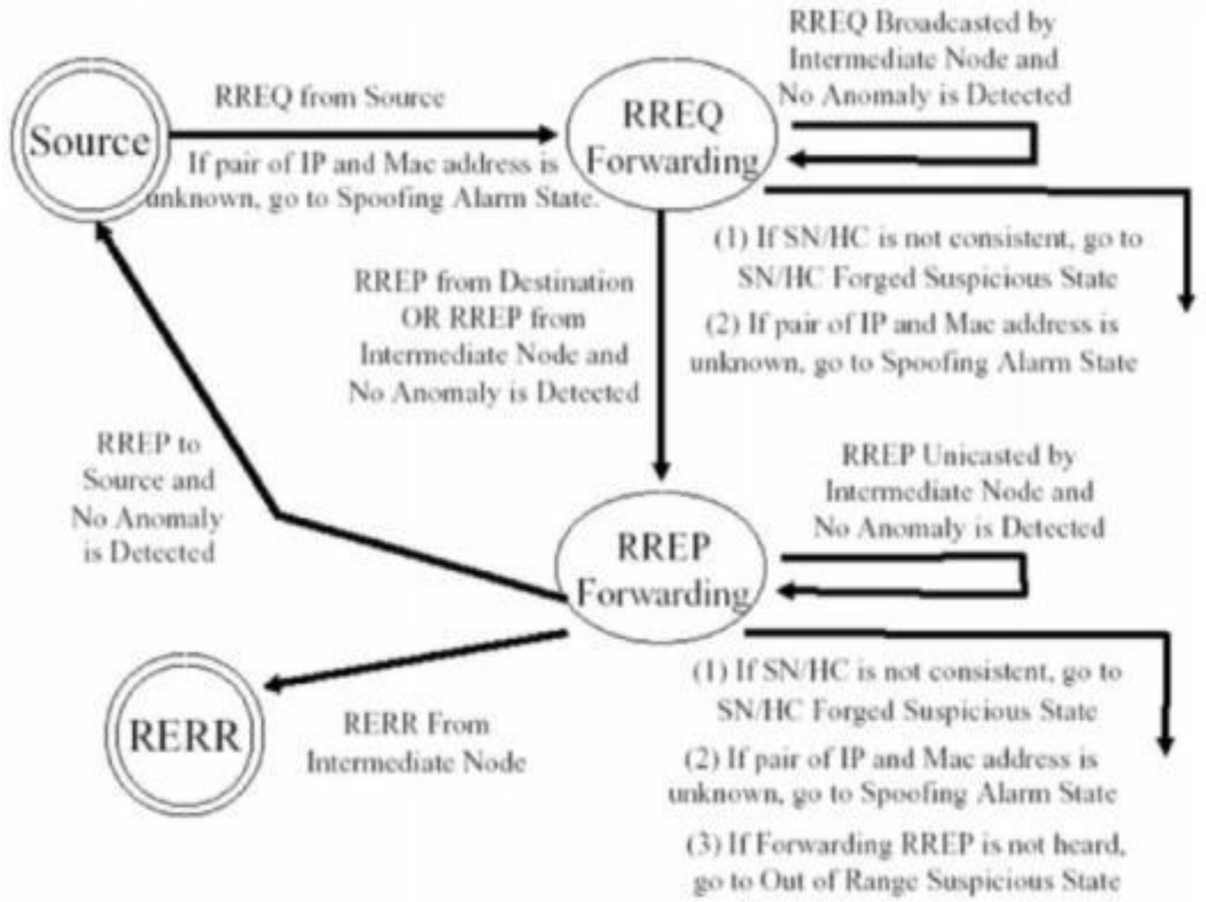


Figure 2. Normal State Diagram for Finite State Machine


Source
RREQ from Source
If pair of IP and Mac address is unknown, go to Spoofing Alarm State.
RREQ Forwarding
RREQ Broadcasted by Intermediate Node and No Anomaly is Detected
(1) If SN/HC is not consistent, go to SN/HC Forged Suspicious State
(2) If pair of IP and Mac address is unknown, go to Spoofing Alarm State
RREP from Destination OR RREP from Intermediate Node and No Anomaly is Detected
RREP to Source and No Anomaly is Detected
RREP Forwarding
RREP Unicasted by Intermediate Node and No Anomaly is Detected
RERR
RERR From Intermediate Node
(1) If SN/HC is not consistent, go to SN/HC Forged Suspicious State
(2) If pair of IP and Mac address is unknown, go to Spoofing Alarm State
(3) If Forwarding RREP is not heard, go to Out of Range Suspicious State

Simulation
Methodology

To better examine the performance of the enhanced intrusion detection system with on-demand routing protocol using hybrid cryptographic techniques for MANETs under different types of attacks, we define three scenario settings to simulate different types of misconduct or attacks.

Scenario

In this scenario, we simulated a simple packet drop attack from the malicious node. The malicious nodes simply drop all packets they receive. The aim of this scenario is to test the performance of the intrusion detection system against limited transmission power and receiver collision.

Simulation Result – Scenario

In this scenario, malicious nodes discard all packets that they pass. The simulation results based on PDR. Proposed scheme improved intrusion detection system with on-demand routing protocol using hybrid cryptography technology for MANETs outperformed Watchdog. From the results, the confirmation-based schemes, including TWOACK, AACK, EAACK, and hybrid schemes, can identify misconduct with limited transmit power and receiver collision. However, if the number of malicious nodes reaches 40%, the proposed system performance will be less than that of TWOACK and AACK. As a result of the introduction of the MRA mode, it takes longer for an MRA confirmation to be received from the target node that the waiting time exceeds the predefined threshold.

Conclusion and Futrure Enhancement

In this article, we have proposed an efficient method of using intrusion detection systems (IDS) located on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. We then described a cooperative game model to represent the interactions between the IDSs in a neighborhood of nodes. The game is defined so that the main goal of the IDS is to monitor the nodes in their neighborhood at a desired level of security to detect abnormal behavior, while the secondary goal of the IDS is to save as much energy as possible.

The assessment of the proposed scheme is done by comparing the performance of the IDS under two scenarios: (a) maintaining the IDS throughout the simulation time and (b) using our proposed scheme to reduce the active time of the IDS at each node in the network. The simulation results show that the effectiveness of the IDSs in the network does not compromise when using the proposed scheme, but that the energy consumption in each of the nodes is significantly reduced, which considerably extends the network life. Here we have adopted a homogeneous network so that all nodes have the same capacities with regard to their computing and energy resources.

References

1. *S. Marti, T. J. Giuli, K. La and M. Baker, "Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment," Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255265, August 2000.*
2. *Manikopoulos and L. Ling, "Architecture of the Mobile Ad-hoc Network Security (MANS) System," Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3122-3127, October 2003.*
3. *K. Nadkarni and A. Mishra, "Intrusion Detection in MANETs - The Second Wall of Defense," Proc. IEEE Industrial Electronics Society Conference '2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.*
4. *Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis,"Secure Routing and Intrusion Detection in Ad-hoc Networks," Proc. 3rd IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March 8-12, 2005.*
5. *N. Marchang and R. Datta,"Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks," Elsevier Ad Hoc Networks, vol. 6, no. 4, pp. 508-523, June 2008.*
6. *Dong, X. Liao, Y. Liu, C. Shen and X. Wang, "Edge Self-Monitoring for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems," vol. 22, no. 3, March 2011, pp. 514-527.*
7. *S. Zeadally, R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.*
8. *N. Marchang and R. Datta,"Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks," IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.*
9. *S. K. Bhoi and P. M. Khilar, "Vehicular communication: a survey", IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.*
10. *Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.*
11. *K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.*
12. *Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.*
13. *Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).*
14. *TIK WSN Research Group, The Sensor Network Museum—Tmote Sky. [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky.*
15. *Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Trans. Instrum.Meas., vol. 57, no. 7, pp. 1379–1387, Jul. 2008.*