An Efficient Intruder Avoidance Method for MANETs

Koppula.Jagadeesh
M.Tech Student,
Department of ECE
Vardhaman College of Engineering (Autonomous),
Shamshabad, Telengana, Hyderabad.

C. Padmini
Assistant Professor (Sr. Grade)
Department of ECE
Vardhaman College of Engineering (Autonomous),
Shamshabad, Telengana, Hyderabad.

ABSTRACT

Among all the up to date wireless networks, Mobile Adhoc Network (MANET) is one amongst the foremost necessary and distinctive applications. Unfortunately, the open medium and remote distribution of MANET create it at risk of numerous kinds of attacks. So, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

In this paper, we define solid privacy requirements regarding malicious attackers in MANET. We propose and implement a new intrusion-avoidance system specially designed for MANETs. Compared to contemporary approaches, it demonstrates higher malicious-behaviour-avoidance rates in certain circumstances while does not greatly affect the network performances.

1. INTRODUCTION

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. This type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self-forming, self-Maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances that most routing protocols in MANETs assume that every node in the network behave cooperatively with other nodes and presumably not a malicious one; attackers can easily compromise MANETs by inserting malicious or non-cooperative node into the network. Due to MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. Hence, it is crucial to develop an intrusion detection system in MANETs. In this paper, we aim to develop such an efficient and reliable intrusion detection system (IDS).

2. BACKGROUND

With the upgrading technology, we are witnessing the expansion of MANETs into industrial application. So it is vital to address its security issues. Such existing IDSs in MANETs are 1) Watchdog 2) TWOACK 3) AACK and 4) EAACK.

MANETs are an appealing technology for many applications such as rescue and tactical operations due to the flexibility provided by their infrastructure. However, this flexibility comes at a price and introduces new security threats. Furthermore, many conventional security solutions used are ineffective and inefficient for the highly dynamic and resource constrained environments where MANETs use might be expected. Unfortunately, the remote distribution and open medium of MANET makes them susceptible to various attacks. For example, due to lack of protection for nodes, malicious attackers can easily capture and compromise the mobile nodes to achieve attacks.

2.1 Watchdog

Watchdog improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked malicious. The major drawbacks are
1) Ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehaviour report, 5) partial dropping and 6) collusion.

2.2 TWOACK

TWOACK overcomes the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. The major drawbacks are 1) Increased overhead 2) Limited battery power 3) Degrades the life span of entire network.

2.3 AACK

Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks are that it suffers from 1) False misbehaviour report 2) Forged acknowledgment packets.

Digital signature

Digital signature is a widely adopted approach to ensure the authentication, integrity, and no repudiation of MANETs. All algorithms except watchdog are based on acknowledgment. Hence, it should be authenticated through digital signature.

2.4 EAACK

Enhanced Adaptive Acknowledgment is designed to tackle false misbehaviour, limited transmission power and receiver collision limitations of watchdog. It involves three parts namely ACK, SACK (Secure ACK), MRA (misbehaviour report authentication). Digital signature is used in EAACK to prevent the nodes from forged acknowledgement attacks. This scheme is explained in detail later.

3. LITERATURE SURVEY

N. Kang, E. Shakshuki and T. Sheltami proposed a scheme called Enhanced Adaptive Acknowledgement (EAACK). This scheme aims to overcome four of the weaknesses in traditional Watchdog mechanism, namely, ambiguous collisions, receiver collisions, limited transmission power and false misbehaviour. But there is no authentication for acknowledgements. The functions of detection scheme largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. So this scheme is not much efficient. Although the simulation result showed that the proposed scheme outputs higher packet delivery ratio, it also has a higher overhead ratio with the increase of malicious nodes in the network. This is due to the introduction of MRA scheme. Elhadi M. Shakshuki proposed EAACK which was designed with the implementation of RSA and DSA digital signatures using DSR routing protocol. Performance evaluation was done and results were obtained. But this EAACK has no provision for handling link breakage and malicious source node scenario. Later the introduction of digital signature to prevent the attacker from forging acknowledgment packets was proposed. It used a new protocol for better security using hybrid cryptographic technique to reduce the overhead caused by digital signature. But it had no provision for handling link breakage and malicious source node scenario. Thus all the existing IDSs have certain disadvantages.

4. PROPOSED METHOD

We introduce an efficient privacy maintain routing protocol that achieves more security by employing anonymous key establishment based on group signature. The setup of this secure routing protocol is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server.

1) Basic routing module

If the source has no route to the destination, then source v initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbour table to find if it has any closer neighbour node toward the destination node. If a closer neighbour node is available, the RREQ packet is forwarded to that node. If no closer neighbour node is the RREQ packet is flooded to all neighbour nodes.

2) Include hacking in basic routing module

In this module Attack issues will arise in to the network. Providing security to the attacks will be considered.

Black hole Attack:

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks.

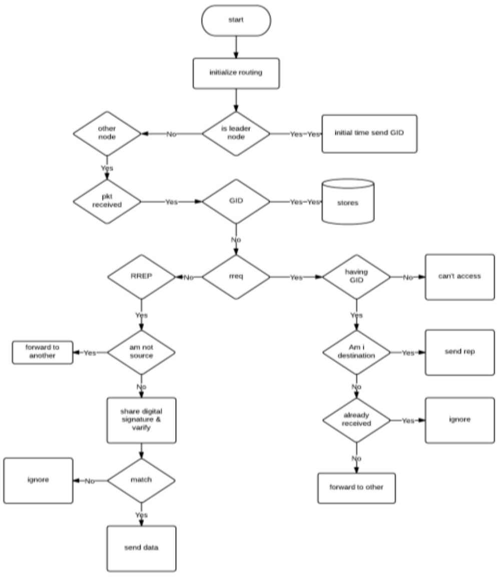
In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

3) Secure Data transmission

In this module Group signature is taken in to consideration for the protection against hacking. Whenever node having the group id/ signature then that node can interact with the other nodes in the network otherwise it cannot interact. In this way the process of avoiding the interaction of hacking node proceeds.

5. ALGORITHM:

```
1. Initialize the nodes as follows
    a. Leader node: (it can share the key at initial time)
    b. Normal node: (normal mobile node)
2. Leader node initially sends the Group ID key to all then mobile node
3. If normal node received that ID then stores into memory
4. If node having GID
    a. It can access the request
5. If not
    a. Can't access the request
6. If node (i) wants to communicate with another node
    a. Node i generates the hash code(by sha-1)
    b. Encrypting (by RSA) that code with private key of node i
    c. And sends to dest… node
7. destination node can verify that encrypted message by using the public key and as well as group ID
    a. if match
        a.i. node j sending own code to source node i
    b. if not match
        b.i. ignore
8. if match code of node j
    a. transfer the data
9. if not match
    a. ignore
```



6. ANALYSIS

Network performance refers to the service quality of a communications product as seen by the customer. There are many different ways to measure the performance of a system, as each system/network is dissimilar in nature and design.

1) Packet delivery function.
PDF is the term used to measure the network performance. PDF defines the how much packet delivered correctly over total number of packet sent

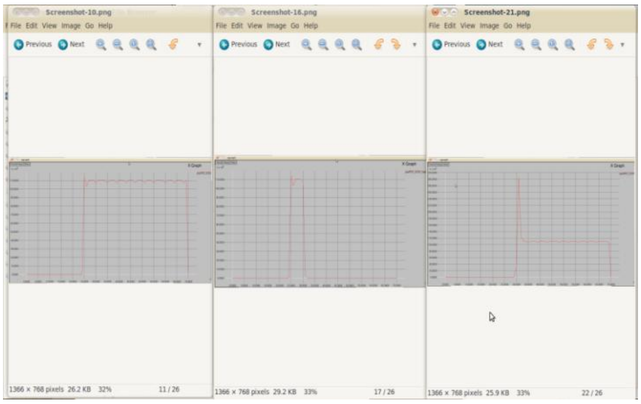
2) Overhead.
Overhead is the one important concept to analyze network performance. Overhead is defined as number of routing and control packet is requiring transferring the data.

7. RESULT

In our project, we analyzed different network environment with main network parameters such as packet delivery radio and overhead.

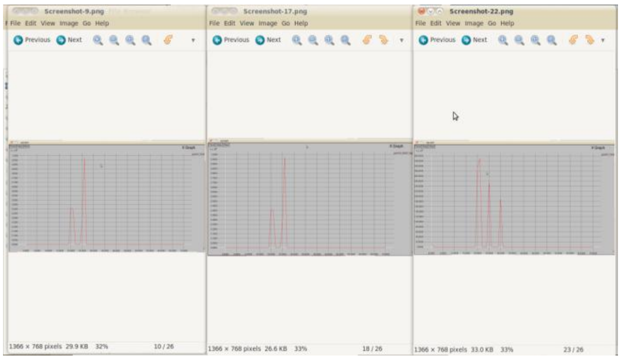
Result shown bellow is packet delivery function. In that graph, there are the three environments (without malicious environment, with malicious environment and SDT environment) shown.

From our result, we can know we improved our network performance


Screenshot-10.png
Screenshot-16.png
Screenshot-21.png
File Edit View Image Go Help
Previous
Next
1366 × 768 pixels 26.2 KB 32%
11 / 26
1366 × 768 pixels 29.2 KB 33%
17 / 26
1366 × 768 pixels 25.9 KB 33%
22 / 26

PDF Comparison b/w AODV, Mali_AODV and SDT

The graph shown bellow is overhead graph, from this result we can know SDT has more overhead than normal AODV. SDT performance is better than normal AODV even overhead is more; the reason is security of SDT is very high so overhead is ignorable in this case.


Screenshot-9.png
Screenshot-17.png
Screenshot-22.png
File Edit View Image Go Help
Previous
Next
1366 × 768 pixels 29.9 KB 32%
10 / 26
1366 × 768 pixels 26.6 KB 33%
18 / 26
1366 × 768 pixels 33.0 KB 33%
23 / 26

OH Comparison b/w AODV, Mali_AODV and SDT

8. CONCLUSION

In this paper, we suggested an secure routing protocol for avoiding intruders in the path based on group signature and ID-based cryptosystem for ad hoc networks. The conception of this method offers solid privacy protection against different types of attacks for ad hoc networks. The protection analysis demonstrates that our method not only provides strong retreat security, it is also less delay and more PDF.

9. REFERENCES

[1] "EAACK-A Secure Intrusion-Detection System for MANETs", Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, 2013.

[2] Securing Ad Hoc Networks, Lidong Zhou and Zygmunt J. Haas.

[3] "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" , Yih-Chun Hu, David B. Johnson and Adrian Perrig.

[4] "On Intrusion Detection and Response for Mobile Ad Hoc Networks", James Parker, Jeffrey Undercoffer, John Pinkston, and Anupam Joshi.

[5] "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan.

[6] "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks", Nidal Nasser and Yunfeng Chen.

[7] "Remote Sensing and Control of an Irrigation System Using a Distributed Wireless Sensor Network", Yunseop (James) Kim, Robert G. Evans, and William M. Iversen.

[8] "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks", Jin-Shyan Lee.

[9] "Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks", Denis Dondi, Alessandro Bertacchini, Davide Brunelli, Luca Larcher and Luca Benini.

[10] "Anonymous Communications in Mobile Ad Hoc Networks", Yanchao Zhang, Wei Liu and Wenjing Lou.