Secure Intrusion Detection in MANETS

Sharatkumar Patangi, Shashank J A, Vikas Murthy T N & Vishal Anant Joshi
Under the guidance of S Lokesh associate professor Department of Computer Science and Engineering, NIE college of Engineering, Mysore, Karnataka

Abstract: The popularity of wireless networks over wired networks has been increasing for the past few decades. The mobility and quantifiability brought by wireless networks makes it preferable for several applications. Among all the present-day wireless networks, Mobile Ad hoc network (MANET) is among the foremost types having important and distinctive applications. Contrast to the traditional network design, MANET will not need a hard and fast network infrastructure; each single node works as a transceiver i.e. it can both transmit and receive. Nodes communicate directly with each other if they’re within the correspondence range of each other. Otherwise, they rely on their neighbors to relay messages. The ability of self-configuring of nodes the in MANETs makes it utmost prominent among vital mission applications like military use or even emergency operations like recovery. However, the open channel and wide dissemination of nodes makes MANETs defenseless against malignant attackers. In this paper, we propose another interruption recognition system named Enhanced Adaptive Acknowledgment (EAACK) uniquely intended for MANETs.

Keywords: Digital signature algorithm Enhanced Adaptive Acknowledgment (EAACK); Mobile Ad hoc Networks (MANET); Digital signature; AACK; TwoACK; Intrusion Detection.

1. Introduction

The recent decades have been the ones with a huge development in the utilization of wireless networks. With decreased expense and exceptional wireless data transmission capacity, wireless networks have shown the capacity to supersede wired networks in various settings. One of the major reasons of interest in wireless networks is its capability of transmitting client information while retaining its mobility. However, this adaptability relies, to a great extent, on the purview of the transmitters. This implies that the members wouldn’t be able stay connected to each other if the separation between them is beyond the scope of the transmitters. Mobile Ad hoc Networks (Manets) tackle this issue by permitting intermediate participants to hand-off information transmission while as of now keeping up versatilit.

Regarding the matter of security in Manets, one of the greatest difficulties is the number of the elements that must be represented: infrastructure less networks, dynamic network topologies, resource limitations and limited physical protections. These qualities make Manets defenseless against both dynamic and inactive assaults. With respect to these difficulties, in this paper, we propose another security component that adopts intrusion detection and cryptography techniques. Each methodology has its own particular qualities and shortcomings. A few of them focus on message authentication and cryptography strategies, yet they experience the ill effects of the late discovery of assaults because of their absence of misbehavior report.

2. Proposed System

The openness of the medium along with the properties such as remote distribution of MANETs make it vulnerable to varieties of attacks. An example, attributable to the nodes’ lack of physical protection, malicious attackers will simply capture the node to harm it. By considering the very fact that almost all routing protocols in MANETs assume that each node within the network behaves hand in glove with different nodes. Presumptively not all the malicious attackers will simply attack MANETs by inserting malicious or non-cooperative nodes into the network. However due to the MANET’s distributed design and ever changing topology, standard centralized observation technique is not any longer possible in MANETs. In the scenarios involving the above mentioned threats, it’s very important to develop associate degree intrusion-detection system (IDS) specially designed for MANETs.

Many of the prevailing IDSs in MANETs adopt associate degree acknowledgment based mostly theme, as well as TWOACK and AACK. The functions of such detection schemes all for the most part depend upon the acknowledgment packets. Hence, it's crucial to ensure that the acknowledgment packets square measure valid and authentic. To deal with this concern, we have a tendency to adopt a
digital signature in our planned theme named increased AACK (EAACK).

Many of the existing Intrusion Detection Systems in MANETs deploy an acknowledgment based scheme, including TWO acknowledged scheme and Adaptive acknowledgement scheme. The functions of such detection schemes all depend on the arrival of the acknowledgment packets. Hence, it is crucial to guarantee the validity as well as the authenticity of the acknowledgment packets. To overcome this problem, we deploy a scheme which uses digital signature and is named as Enhanced AACK (EAACK).

Advantages of Proposed Systems are:
1. No false misbehavior
2. Receiver collisions can be avoided
3. Transmission power consumption is less

3. Network Topology

A topology as above is considered. The topology contains of four nodes, namely, 192.168.0.1 to 192.168.0.4. The node 192.168.0.1 cannot access the node 192.168.0.4 directly and conversely. Similarly, the node 192.168.0.2 and 192.168.0.3 should be reached with the help of the intermediate nodes. The node 192.168.0.1 in order to find an optimal path to 192.168.0.4, sends a Route Request packet to its neighbours. The neighbour nodes will forward it to its neighbours. This implies that node 192.168.0.4 receives two Route Request packet, one from 2 and one from 192.168.0.3. The fastest among the two is chosen as the optimal path and the destination node 192.168.0.4 unicasts a Route Reply packet with that path to the sender 192.168.0.1.

4. Implementation Details

The implementation of the approach is broadly divided into three functionalities. They are,

- Fake acknowledgement
- Drop packets
- Fake misbehavior authentication

An optimal path between source and the destination is found out by the means of route discovery. This includes flooding of RouteRequest packet throughout the network until the destination is reached. Upon receiving the request packet the destination replies back to the source. The first packet which arrives at the source node is the optimal path between the source and destination. Further transaction are carried out via this packet itself.

4.1 Route Discovery

This module uses an on demand routing protocol to calculate the shortest path between the source and destination. It uses Dynamic Source Routing (DSR) algorithm to calculate the optimum path.

For this purpose, a route discovery packet is created. This packet is then broadcasted to all the neighbours using UDP protocol. A node on receiving the packet checks if it the destination being searched for. If it is, then it sends back an acknowledgement. If it isn’t the destination, then it forwards the packet to its neighbouring nodes.

4.2 Data Transmission
This is the most important module. Every node uses TCP protocol to send a packet to the next node. All transmissions are one-to-one. This adopts end-to-end acknowledgement to confirm the delivery of a packet. Every acknowledgement is digitally signed by the sender, using a pre-shared key (Symmetric Key Algorithm). Also, selective repeat protocol is used. In case of a failure, the packets for which no acknowledgement has been received before the timer runs out, those packets are retransmitted.

The timer is calculated dynamically. The wait time to receive an acknowledgement is changed (increased or decreased) each time a packet is sent.

4.3 Acknowledgement Transmission

This module uses a 2-acknowledgement scheme where, one acknowledgement is from the neighbour, on successfully receiving the packet and other acknowledgement is from the neighbor node which is neighbor to the neighbor node. On receiving the two acknowledgements, it can be checked if the next node is transmitting the packets or not.

4.4 Misbehavior Report Authentication

A node might send a misbehaviour report to its neighbour. To ensure that no fake MRA is generated, the nodes digitally sign the reports. This ensures that there are no fake MRAs being generated. Now, the neighbour uses a different path (optimal) to confirm the malicious behaviour claim.

4.5 Attack Prevention

Once a malicious node has been detected, its presence is broadcasted across the network. This information is also used to calculate a new optimal path. All the nodes now will have to update its respective routing tables. All the nodes which were using the malicious node as its route to the destination will now have to re-route further packets through another route which is clean of any malicious nodes.

5. Conclusion

Using this system or the solution the task of finding an intruder node can be found out effectively without any flaw. In doing so, the MANETs environment can be considered as safe as infrastructure based architecture. The approach helps us to achieve at most security in situation such as fake acknowledgement, fake MRA and drop packets. In drop packets the sender node chooses an alternative optimal path rejecting all the paths which containing malicious node. During the fake acknowledgement problem, this system enters into defense mechanism by deploying two acknowledgement scheme there by helping us to find the intruder node easily. The situation involving fake MRA can be easily verified as it involves usage of digital signature. Since only the authenticated nodes can digitally signature, fake MRAs don’t stand a chance.

6. Future Enhancements

The above mentioned approach helps us in detecting the malicious nodes which are not authorized. This must be extended to authorize nodes as well since information disclosure is a major threat to the manets.

7. References