Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancing the Secure Data Transmission for Routing Attacks in MANET

Vijayakumar.P , Tamizharasan.P
Department of Information Technology,
V.S.B Engineering College, India

Abstract - Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. MANET has been normally deployed in the network to avoid the routing attacks. In existing solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. Each node in MANET plays a router role while transmitting data over the network. While we transmitting the data over the network the Whole file can be divided into different packets. Attacks can be further categorized as either outsider or insider attacks. The target attacks could be also divided into data packet or routing packet attacks. With routing packet attacks, attackers could not only prevent existing paths from being used and also spoof non existing paths to lure data packets to them. Which have been carried out on modeling MANET routing attacks using routing table recovery. The routing table recovery which intimates the intrusion response to the receiver.

Keywords—Mobile Ad- Hoc network, fuzzy, dempster-shafer theory.

I. INTRODUCTION

A collection of interconnected nodes is said to be Network. It classifies as wired, wireless or wired cum wireless. An ad-hoc network is a self-configuring infrastructure less network. Within the certain range All wireless enabled devices can discover and communicate each other in a peer-to-peer fashion without involving central access points. The Unique characteristic of MANET is the dynamic nature of its network topology this would be frequently. Each mobile node in MANET plays a router role while transmitting data over the network with multiple nodes. The intrusion responsive actions in MANET by isolating uncooperative nodes based on the node reputation derived from the behavior of the each node in the particular network. Furthermore a simple response against malicious nodes often neglects possible negative side effects involved with the response actions of the nodes. The improper countermeasures may cause the unexpected network partition and bring the additional damages to the network infrastructure. The concept of mobile ad-hoc network is dynamic and depends upon the movement of the nodes so it can change unexpectedly and rapidly.

The way of risk assessment is still a nontrivial and challenging problem due to its involvements of subjective knowledge and objective evidence and the logical reasoning because the Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation of the certain network. A naive fuzzy cost-sensitive intrusion response solution for MANET. Total cost of the model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. We seek a way to bridge this gap by using Dempster-Shafer mathematical theory of evidence (D-S theory), which offers an alternative to traditional probability theory for representing uncertainty Network routing protocol designing because sometimes data has to be transmitted within real time constraints.

Characteristics of MANET

- In MANET each node acts as a router and forwards the packet to destination. That is it is autonomous in behavior.
- MANET does not depend on any preexisting infrastructure.
- The nodes can join or leave the network an anywhere at any time, making the network topology dynamic in nature.
- Communication is via wireless means(generally via radio waves)
- Mobile nodes are classified with less memory, power and light weight features.
- Each node can perform the roles of both hosts and routers.

Challenges in MANET

Limited power supply is the biggest challenge of an ad- hoc network so if we want to increase the network lifetime (duration of time when the first node of the network runs out of energy) as well the node lifetime then we must have an

energy efficient protocol. Hence an ad-hoc routing protocol must meet all these challenges to give the average performance in every case.

In MANET routing packets in an environment where the topology are changing frequently. Vulnerability is one of the main weakness compare to wired network. The main challenges in mobile ad-hoc5 networks are as follows:

Dynamic topology

In mobile ad hoc networks the nodes may leave and join the network randomly. This forms a network with dynamic topology. Due to the absence of fixed infrastructure it is difficult to distinguish between trusted and non trusted nodes also the intruder would be able to join the network easily and carry out his/her attacks.

Cooperativeness

Nodes of a MANET are highly cooperative for transferring information and routing messages. This leads to the target of several new attacks. For example, a malicious node acts as a neighbor to the legitimate node and involves in decision making process. This process significantly affects the entire network.

Shared radio channel

The shared transmission media is highly susceptible to link attacks, which include passive eavesdropping and active interfering with the leakage of secret information and data tampering, impersonation, message replay, message distortion, and denial of service (DoS). Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, inject erroneous messages, modify messages, and impersonate a node, thus violating availability, integrity, authentication, and no repudiation.

Limited resource availability

Nodes of mobile ad hoc network use a battery power to operate. Nodes may be laptop and PDA or mobile phones with the computational and storage capacities of these devices may vary. Varying capacity of nodes results in drop of packets to save its resources. The intrusion detection system must take into account limited resources.

Backdrop Clear Line of Defense and Secure Communication

MANETs do not have a clear line of defense. There is no central authority to install an access control system. In some cases a cluster head having an IDS system. In many cases the clusters head may subject to attack.

II. PROTOCOLS USED IN MANET

Routing is the process of information forwarding packet towards its destination using most efficient path. Routing is the mechanism of information exchange from one host to the other host in a network. the help such metric like Number of hops, traffic, security Efficiency of the path is measured. In Ad-hoc network every host node acts as specialized router itself. In MANET routing protocols can be categorized into following.

- Proactive routing protocol
- Reactive routing protocol
- Hybrid routing protocol

Proactive routing protocol

Each node in this routing protocol maintains. Information of only active paths to the destination nodes.In this protocol each node sends a broadcast message to the entire network if there is a change in the network topology. Each proactive routing protocol keeps one or more tables representing the overall topology of the network. These tables are updated continuously in order to maintain up-to-date routing information from every node to each other node. The routing information is maintained up to date; topology information needs to be exchanged between the nodes on a regular basis leading to reasonably high overhead on the network. In additional, the routes will also be available on request. Most of the proactive protocols begin from conventional link state routing with the Optimized Link State Routing protocol (OLSR).

Reactive routing protocol

Reactive routing protocols are Dynamic Source Routing (DSR) or Ad hoc On-Demand Distance Vector (AODV). In on-demand routing the routes to destinations are discovered only when the source node has a packet to forward, thus, have lower routing overheads.IN DSR source routing protocol data packet carries the route information from source to destination. DSR is the basic mechanisms of Route discovery and route maintenance. A Route Request is sent to all the neighbor nodes when source node wants to establish a route. The neighboring nodes on receiving the request update themselves on the source route and forward it to their neighbors.

Hybrid routing protocol

Hybrid routing protocols aggregates a set of nodes into zones in the network topology. Where the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. The reactive approach is used to route packets between different zones. Hence, in hybrid schemes, the route to a destination that is in the same zone is established without delay and a route discovery and a route maintenance procedure is required for destinations that are in other zones in the network. The zone routing protocol (ZRP) and zone-based hierarchical link

state (ZHLS) routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes and the frequency of topology change.

III. ROUTING ATTACKS

Attacks in MANET can be categorized into

- Passive attack
- Active attack

Passive attack

This attack does not actually disrupt the operation of the operation of the network. Example: Snooping is unauthorized access to another person's data.

Active attack

This attack attempts to alter or destroy the data being exchanged in the network

Layer based attack

Network Layer Attack is classified into different types of attacks on network layer is discussed hereby:

Wormhole Attack: This attack where a malicious node will receives packets at one location in the network and tunnels them to another location in the network, hence these packets are resent into the network. So this tunnel between two colluding attackers is referred to as wormhole.

Black hole Attack: In this an attacker listen the requests for the routers in a flooding based protocol in the network. When the attacker receives a request for a route to the destination node and it creates a reply consisting of an extremely short route and enters into the pathway to do anything with the packets passing between them.

Byzantine Attack: This attack is a compromised intermediate node or an asset of compromised intermediate nodes works in collision and which carries out attacks such as creating routing loops and forwarding packets on non-optimal paths and selectively dropping packets which result in disruption or degradation of the routing services.

Replay Attack: In this attack an attacker that performs a replay attack is retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. Hence this attack usually targets the freshness of routes, and then can also be used to undermine poorly designed security solutions.

Denial of Service attack: This attack aims to attack the availability of a node or the entire network without any delay. If the attack is successful then the services will not be available. Hence the attacker generally uses radio signal jamming and the battery exhaustion method.

Quality of Service

The widespread use of mobile and handheld devices is likely to popularize Ad-hoc networks which do not required any wired infrastructure for intercommunication. The nodes of mobile Ad-hoc networks operate as end hosts as well as routers. They inter communication through single-hop and multiple-hop in a peer –to- peer fashion. With the expanding scope of applications of MANET's, the need to support Quality of Service in these networks is becoming essential. Quality of Service QoS is usually defined as a set of service requirements that needs to be met by the network while transporting a packet of stream from a source to its destination .The network is expected to guarantee a set of measurable prespecified service attributes to users in terms of end-to-end performance, such as delay, bandwidth ,probability of packets loss, and delay variance(jitter) .power consumption and service coverage area are two other Quality of Service attributes that are more specific to MANET's.

MANET's are likely to expand their presence in future communication environments. Support for Quality of Service will thus be an important and desirable component of MANET's. Although difficult, it is quite interesting and challenging to design and develop Quality of Service provisioning techniques for MANET's. Quality of Service plays an important role for providing QoS in wireless ad-hoc networks. The major goals of QoS routing are in general twofold manner which are,(1)Selecting routes with satisfied QoS requirement(s).(2)achieving global efficiency in resource utilization. In this area we first discuss some key design considerations in providing QoS routing support and present a review of previous work addressing the issue of route selection subject to QoS constraint(s). We then devise an on-demand delay – constrained unicast routing protocol used in the network. Hence various strategies are employed in the protocol to reduce the communication overhead in acquiring cost-effective delay-constrained routes in the network. Simulation results are used to verify our expectation of the high performance of the devised protocol. QoS routing is an essential component of a QoS architecture .In QoS routing ODRP support cost effective bandwidth constrained routing in wireless and Ad hoc Networks. Here I provide some topics that fall into the area of QoS routing in Ad hoc Networks.

- Scalability
- Integration with other Network components
- QoS Multicast routing
- QoS Routing with Power control

IV. PREVIOUS WORK

Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Each such simple response against malicious nodes often neglects possible negative side effects involved with the response actions and the effects. In MANET, the improper counter measures may cause the unexpected network partition which will bring the additional damages to the network infrastructure. Hence to address the above-mentioned critical issues more flexible and adaptive response should be investigated. But the notion of risk can be adopted to support more adaptive responses to routing attacks in MANET. Subjective knowledge could be retrieved from the previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation and the idea. Wang et al. proposed a naı¨ve fuzzy cost sensitive intrusion response solution for MANET. Hence their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning.

Disadvantage

The risk assessment is still a nontrivial and a challenging problem due to its involvements of subjective knowledge with the objective evidence and logical reasoning. Hence it will take more time to send data from sender to receiver because the whole files transmit through single node.

V. PROPOSED WORK

The MANET Architecture Shows the Model of MANET Network. In this network describes the communication the server, Intermediate and Client. The Sender have the file and it uses the File Splitting and random number generation. X1, X2, X3 are the splitted packets with random number. In the Router have the routing table To store the routing values. The Modified file values also stored in the Routing tables. The Receiver will receive the X1, X2, X3 files and combine the Different and uses the **Routing table Recovery** technique to know the routing values. And Find the Anomaly detection Using **Dempster-shafer theory** to compare the Packet values With the Routing table values.

Advantage:

The true data can be sending from sender to receiver through different intermediate node or router. So it will take less time to send data. Routing attacks can be found with the help of random value change.

Extended dempster-shafer theory of Evidence

The Dempster-Shafer mathematical theory of evidence is both a theory of evidence and a theory of probable reasoning. Hence the degree of belief models the evidence with the Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidences. Though, previous research efforts identify several limitations of the Dumpster's rule of combination

1. **Associative For DRC**:The order of the information in the aggregated evidences does not impact the result.

2**. Nonweighted DRC:** This implies that we trust all evidences equally. Conversely, in reality, our trust on different evidences may differ. In other terms, it means we should consider various factors for each evidence.

VI. SYSTEM ARCHITECTURE

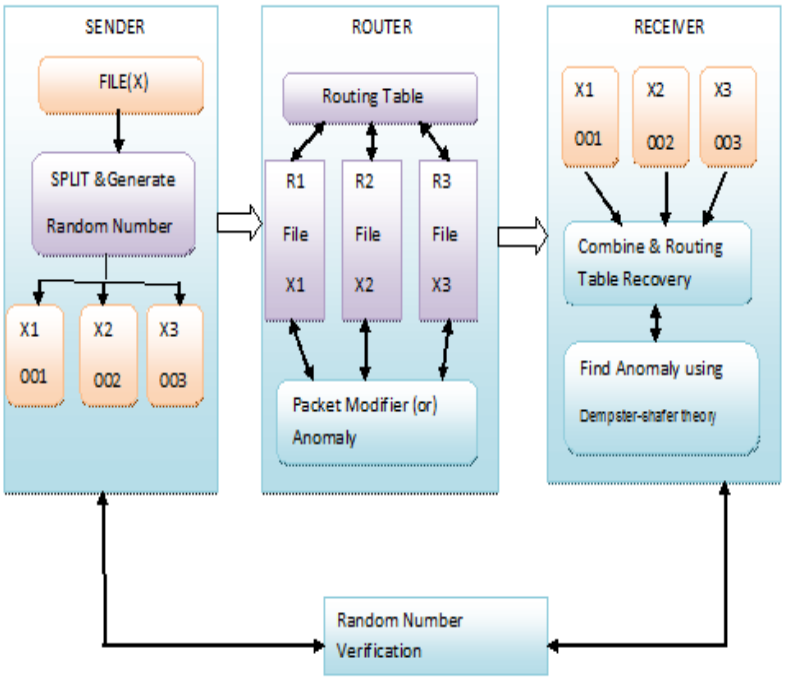

Figure 1.0 Secure Data Transmission

1. The sender can send the file by splitting the file into number of packets. This uses the Packet splitting algorithm.
2. The sender will send the packets with the Key value and Intermediate router IP. The Key value will be generated by using key generation algorithm. The packets, Key and Intermediate receiver IP are encrypted and send to intermediate receiver.
3. The Packets will receive into different intermediate client. If the receiver is changing the packets then the packet value will be changed in the routing table. The intermediate client will be a hacker.
4. The modified file packets will send to receiver. The receiver will merge the file by using packet marking Key. The Routing table has the different routing value s for the corresponding packets from the different intermediate receiver IP.
5. It Will Compare the Routing table values with the Packet marking values If both the values matches the client can download the Original file else they can find the hackers.

VII. CONCLUSION

MANETs is an emerging technological field and hence is an active area of research. Since of ease of deployment and defined infrastructure less feature these networks find applications in a variety of scenarios ranging from emergency operations and disaster relief to military service and task forces in the certain area. In this paper we have proposed a risk aware solution for mitigating MANET routing attacks .mainly our approach consider the secure data transmission against the routing attacks. It is based on the Dempster-Shafer theory of evidence with notion of importance factor. This identifies the routing attacks as well as finding attacked node while transmitting data. Using both the table recovery and packet marking data to be sent in less time and secured way. It will leads to finding the network risk.

REFERENCES

[1] Rusha Nandy, Debdutta Barman Roy" Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011).

[2] Ziming Zhao, Gail-Joon Ahn, "Risk-Aware Mitigation for MANET Routing Attacks", IEEE transactions on dependable and secure computing 2012

[3] Kartik Kumar Srivastava, Avinash Tripathi", Secure Data Transmission in MANET Routing Protocol",Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921.

[4] PriyankaGoyal, Vinti Parmar,Rahul Rishi" MANET: Vulnerabilities,Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

[5] Lili Sun, Rajendra P. Srivastava," An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions".

[6] Yan Lindsay Sun, Zhu Han," Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", IEEE journal on selected areas in communications, vol. 24, no. 2, february 2006.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector routing," Mobile Ad-hoc Network Working Group,vol. 3561, 2003.

[8] Amit Shrivastava, Aravinth Raj Shanmogavel,"Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols".

[9] Abhay Kumar Rai, Rajiv Ranjan Tewari," Different Types of Attacks on Integrated MANET-Internet Communication".

Mr.P.Vijayakumar Pursing the M.Tech (IT) in V.S.B Engineering College. He has received B.E (CSE) degree from Angel College of Engineering and Technology. He has total number of 4 publications, 1 paper in International conference and 3 papers in national conferences and participated in various symposiums and workshops held at different places. His area of interest includes Wireless Network Mobile computing and Data Structures.

Mr.P.Tamizharasan has received the B.Tech (IT) degree from Anna University and M.Tech (IT) degree from Dr M.G.R Educational and Research Institute. He is currently working as an assistant professor in V.S.B Engineering College. His area of interest includes Network Security, Data Mining and Steganography, MANET.