IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 46-52
www.iosrjournals.org

A Secure Wireless Transport Layer for MANET

Mr. P.S. Sujith Kumar, Dr. J. Frank Vijay
Ph.D – Scholar, Department of CSE, Hindustan University, Chennai. sujithkumar@sngce.ac.in
Professor & Head, Department of I.T.,KCG College of Technology Chennai. hodit@kcgcollege.com

Abstract: *MANETs is a type of ad hoc networks that can change the locations and configure itself on the fly. Main unique features are open communication channels, dynamic network topology, limited device capabilities bandwidth and lack of infrastructure or central administration support etc have made secure efficient and reliable end-to-end operation in manet is a challenging task. The primary focus of this paper is to provide transport layer security for end-to-end communication through data encryption. The proposed model provides, authentication, privacy, integrity and also to protect against denial of service(DoS) attacks. Hence this is found to be a good security solution in the networks.*

I. Introduction

MANETS is an emerging technology in the recent areas because of the demand to use the mobile phones in our daily life. As the users who are using the mobile are not stable at one place [1]. There emerges a technology to carry out an effective communication between two nodes where the infrastructure is not available, impractical or expensive. The MANET use wireless networks to connect with different nodes. (See Figure (1))

Figure (1): Mobile Ad hoc Network (MANET) sample.

These networks configure themselves even though they are not connected to any wireless routers. The mode of communication used by MANET is radio frequency in air to transmit and receive any data instead of using any physical hardware. Applications of MANET in real world is amazing and have been used in many critical situations. An ideal real time application of MANET is search & rescue operations.

Fig – 2 – Search & Rescue Operations

II. Basic Architecture of MANET

Fig – 3 Rescue Operations in Remote Area

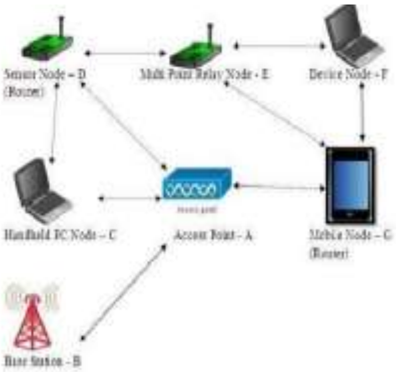

Fig – 4 – Basic Architecture of MANET

Assume a place where a search & rescue operations are carried out as shown in Figure – 3 where there is no proper infrastructure or it has been totally destroyed or perhaps the region is too remote. So, the rescuers have to make communication with the nodes to carry their job as shown in Fig -
2. They can automatically establish a data network with the communication equipments. Another commercial application of MANET is Ubiquitous computing where network may be made more widely available and easier to use. There are lot of applications already in existence when MANET's are considered. However, MANET's are not perfect. There exists a lot of challenges which has to be analyzed in depth for further understanding & research. This paper presents an overall insight in analyzing the various challenges of MANET like mobility, scalability, bandwidth limitations & power constraints.

In MANET each node itself is a router for all the packets coming from or going to the other nodes[13]. In Fig – 4, there are seven nodes in the wireless networks (Node A, Node B, Node C, Node D, Node E, Node F & Node G). Node D can get the incoming packets from Node E, Node F, Node G & Node A. Node D can send packets to Node C & Node A or Vice versa. Here, the nodes act themselves as mobile & therefore, the bandwidths available to any node at any instant are variable. So, because of this each wireless link in MANET provides a limited bandwidth. MANET communication is multihop. For example, if Node D wants to transmit packet to Node G, it is done through these three steps.

1. Node D – Node E
2. Node E – Node F
3. Node F – Node G

III. Challenges of MANETs

a. Bandwidth Limitations

The Capacity of the wireless links is always less than the wired links. Bandwidth is a main attribute of MANETs to determine the data rate available on a network route.

b. Clusters

In MANETs, nodes form a cluster in a wireless networks. Each nodes which are distributed inside the networks acts itself as a host or a router. So, because of this dynamic topology there are various security threats to this MANET architecture.

c. Routing

Routing is one of the important challenges of MANET. In MANET, the router connectivity may change frequently, leading to the multi – hop communication paradigm that can allow communication without the use of base station. Routing is one of the core problems of networking for delivering data from one note to the another.

d. Topology

Nodes in MANETs are free to move in an environment to establish link between them. So, there is a need to maintain a trust relationship between notes when they are communicating with each other to forward packets in the network.

e. Node Sustainability

Nodes at MANET has less CPU Capability, low power storage & small memory size at many cases. A strong algorithm should be developed in low power consumption so that the battery consumption will be less during the forwarding of packets.

IV. Literature Analysis

A vast analysis has been made for finding the problems encountered in MANET and found the following[11,12,14,15]:

a. As the nodes in the MANET communicate each other which is present in the coverage area, then arises a question of **how to maintain the trust relationship between nodes?**
b. In MANET, as the routing is very dynamic nature, then what are the ways to eliminate routing overhead?
c. What are the ways to avoid the frequency of packet losses in wireless networks?
d. MANET's do not have a centralized router to support communication and each node in the network has to act as a router as well.

Success of MANET Technology:-

–A MANET can exist and work if and only if the participating nodes behave in a co- operative manner wherein the data packets of other nodes are forwarded faithfully.‖

But, the problem arises due to the following factors:-

I. The network topology in MANET is dynamic due to the mobility of nodes leading to the change in the connectivity among the nodes.
II. The connectivity of the nodes varies with the time due to departure or arrival of nodes in the network.
III. MANETs are vulnerable to black hole attacks launched by malicious nodes.
IV. MANETs are vulnerable to grey hole attacks launched by selfish nodes.
V. With the time, the nodes which were earlier cooperative may become selfish due to loss of power.

All the features of MANETs design is a challenging task even today. There has always been the need for efficient protocols which enable the nodes to communicate without centralized routers. These complex issues have posed many open problems for researchers and provided them opportunities for making significant contributions to this area.

V. Routing in MANETs

The initial routing protocols used in MANETs such as AODV, DSR, WRP & DSDV were focused mainly on the routing process and were devoid of security mechanisms. All the protocols have the basic assumption that all nodes will forward the packet faithfully. **But, this condition is very idealistic and it wont often exist in MANET.**

The initial security protocols used in MANSETs such as ARAN, ARIDANE, SAODV, SPINS & SRP were based on conventional encryption techniques where in the data are encrypted before transmission so that the data can be prevented from malicious nodes. These way of transmitting data in the network is not successful due to the following reasons:-

a. Encryption process in quite expensive.
b. The major stress lies on the data and not on the route.
c. The route should be secured before protecting the data in the network.

The advanced security mechanisms have been identified by the researchers by the name trust based protocols[7,9,10]. The example of this protocol includes CORE, CONFIDANT, SAR, WATCHDOG, PATHRATOR & OCEAN. In these protocols, the behavior of the node will be decided based upon the information given by other nodes. Based on this, a trust index will be created[8]. This type of protocols suffered from the following fundamental drawbacks:-

a. At the initial stage of operation, how a node will trust other nodes?
b. The entire trust will be build only after some time period.

Thus, the MANET architecture suffers from these two main drawbacks.
1. The encryption based techniques provide security to the data and not to the route.
2. The trust based mechanisms are unable to provide head start to the network.

VI. Problem Defined

Keeping the above problems in mind, the problem definitions have been framed as follows:
i. A protocol can be developed by using the public key cryptographic technique without giving any burden to nodes.
ii. The purpose of cryptography should secure the route as well as data.
iii. Trust model should be developed from the initial start state in the network.
iv. The Protocol should be intelligent to:-
a. Adapt varying time limitations.
b. Adapt varying security requirements.
c. Deal with malicious nodes

VII. Objective of Research

The main objective of our research focuses on developing the protocol with the following characteristics:
a. First hand trust should be given the preference in the initial stage and it should be steadily mixed with second hand trust with the passage of time.
b. Adjustable security requirement according to the sensitivity of the data.
c. The network remains operational in presence of malicious nodes (Availability) and selfish nodes.

VIII. Protocol Design

We have assumed that the ad hoc network is a managed one where there is a deploying agency that issues the basic guide lines to the nodes entering/ leaving the ad hoc network while designing the protocol. The agency doesn’t interfere in the routing process and other routine activities of the network[3]. This is our way of maintaining the purity of the ad hoc concept and at the same time providing the system with basic guide lines of operation so as to address security and other issues.

The security mechanism incorporated in the proposed routing protocol is based upon the trust/ reputation concept. As discussed earlier, it takes time for the trust index to grow to a requisite level before it can be used for believing a node for its benevolent behavior. To give a head start, in such a scenario, we have introduced a new concept called ―AuthBook‖[6]. This was used wherein the nodes use authentication response mechanism for authenticating each other. This ensures a secured environment right from the beginning. This also provides a way to secure the route (not data) through cryptography

The protocol contains the provision for periodic sharing of power status so as to identify potentially selfish nodes. Such nodes are given due regards as they are different from malicious nodes and their packets are forwarded for some limited times. Based on the observed behavior the nodes are classified into the following categories: black listed selfish, trust worthy, high trust worthy. The routes are created keeping in view the security requirement of the data and accordingly choosing the class of intermediate nodes. To accomplish this, a rule base was designed that makes the routing protocol an intelligent one that can adapt as per the requirement of the situation.

For the speedy growth of the trust it is mandatory that the trust information be shared between the various nodes of the network. Such information is known as second hand trust information. While incorporating the second hand trust, the class of the node supplying the trust information was checked[4]. If the node was blacklisted the information was rejected. A proportionate weightage was given to other classes of nodes. While designing the proposed protocol, **the base protocol taken was AODV.**

IX. Protocol Performance Evaluation

To evaluate the performance of the designed protocol we choose NS2 Simulator to ensure that the protocol performance has been properly checked and evaluated[2]. The performance of the designed protocol will be evaluated based on the following metrics:-

Packet Delivery Ratio (PDR): Defined as the ratio of number of packets received by the destination to the number of packets sent by the source.
Delay: Defined as the time taken by the first data packet to reach to the destination sent by the source node.
Throughput: Defined as the number of bits per second received by the receiver sent by the source node.
Hop Count: Defined as the total number of intermediate nodes to reach from source to destination node.
Probability of Reachability (PoR): Defined as every fraction of possible reachable routes to the all possible routes between all different sources to all different destinations.
Network Lifetime: Defined as the time in which K% of the nodes becomes dead.
Jitter: Occurs when in a transmission scenario different packets take different amount of time in reaching from source to destination. Jitter can be measured by using the standard deviation of packet delay. If a communication system has large amount of jitter then the signal quality is very poor.
Successful Route Formation: Percentage of route formed successfully to the number of route requests generated by the source.

X. Protocol Implementation & Simulation

The implementation of the protocol was done in ns2 by making the suitable modifications in the program modules. The basic parameters used in the simulation process are given in Table 1.

Examined Protocols	AODV, AODV$_n$
Simulation Time	30 – 2000 sec
Energy Model	Mica – Motes
Communication Model	IEEE 802.11
Battery Model	Linear
Data Rate	1 Mbps
Default Battery	1200mah

Table 1 – Simulation Parameters

The Simulation traces were analyzed, the following are the observations noted:-

Data packet delivery ratio: Figure 5 shows Data packet delivery ratio versus speed for the studied protocols. It is clear that packet delivery ratio is very close to 1 at speed 0 m/s for all protocols. However, as speed increases, the ratio decreases dramatically.

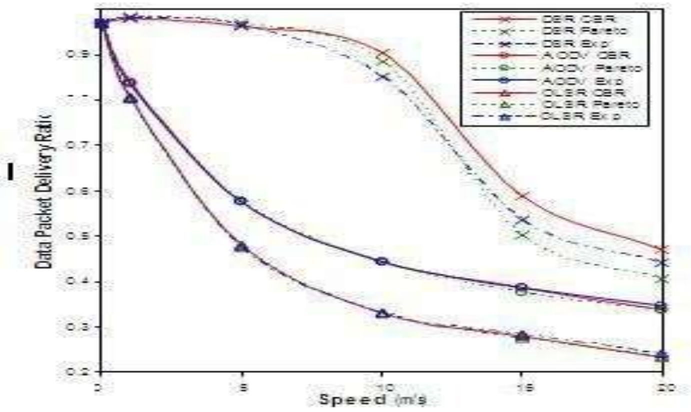

Fig – 5 – Data Packet Delivery Ratio Vs Speed

<u>Throughput (messages/second)</u>: Figure 6 shows the throughput of the protocols measured in messages/second versus speed. AODV has maintained a high throughput at speeds less than 10 m/s.

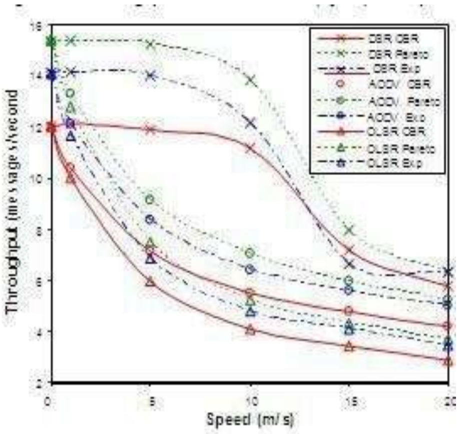

Fig – 6 Throughput Vs Speed

XI. Limitations & Assumptions

The following limitation and assumptions were made for simulation purpose:

i. Each node declares its residual battery correctly.
ii. Malicious node works in individual manner and not in groups.
iii. Participating nodes cannot modify the structure of packets.
iv. Protocol tested in simulation and not in real.

XII. Conclusion

This paper resembles an effort to re- examine the existing protocols in the presence of statistically self-similar traffic model. The proposed WTLS to defend againt DoS attack and it also provides authentication,privacy and integrity of packets in transport layer of manets. we have got a positive result when compared with other models. As a continuation of this research work, it would be very interesting if we further evaluate this protocol to address the problems in depth in real time environment.

References:-

[1] Y. Hu, A. Perrig and D. Johnson, ―Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,‖ Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, September 2002, pp. 12-23. doi:10.1145/570645.570648.

[2] K. Sanzgiri, B. Dahill, B. Levine, C. Shields and E. Belding-Royer, ―A Secure Routing Protocol for Ad Hoc Networks,‖ The 10th IEEE International Conference on Network Protocols (ICNP), 12-15 November 2002, pp.78-87.

[3] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C.Shields and E. M. Belding- Royer, ―Authenticate Routing for Ad Hoc Networks,‖ IEEE Journal on Selected Area in Communications, Vol. 23, 2005.

[4] Y. Hu, D. Johnson and A. Perrig, ―SEAD: Secure Effi- cient Distance Vector Routing in Mobile Wireless Ad Hoc Networks,‖ The 4th IEEE Workshop on Mobile Com- puting Systems and Applications, June 2002, pp. 3- 13.

[5] P. Papadimitratos, Z. Haas and P. Samar, ―The Secure Routing Protocol (SRP) for Ad Hoc Networks,‖ 2002.

[6] D.Johnson, D. Maltz, and Y.-C. Hu, ―The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),‖ IEEE Internet Draft, April 2003.

[7] C. E. Perkins and E. Royer, ―Ad-Hoc On- Demand Dis- tance Vector Routing,‖ Proceedings of 2nd IEEE Work- shop on Mobile Computing Systems and Applications, 1999, pp. 90-100. doi:10.1109/MCSA.1999.749281

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, ―Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,‖ Pro- ceedings of the 6th Annual International Conference on Mobile Computing and Networking (ACM MobiCom 2000), New York, 2000, pp. 255-265.

[9] S. Buchegger and J. Y. Le-Boudec, ―Nodes Bearing Gru- dges: Towards Routing Security, Fairness, and Robust- ness in Mobile Ad Hoc Networks,‖ Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-Based Processing, Canary Islands, 2002, pp.403-410.

[10] S. Buchegger and J. Y. Le-Boudec, ―Performance Analy- sis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-Hoc Networks,‖ Proceedings of MobiHOC'02, June 2002, pp. 226-236.

[11] P. Michiardi and R. Molva, ―CORE: A Collaborative Reputation Mechanism to Enforce Cooperation in Mobile Ad-Hoc Networks,‖ In: J.- B., Borka and K. Tomaz, Eds., Advanced Communications and Multimedia Security, Kluwer Academic Publishers, 2002.

[12] S. Bansal and M. Baker, ―Observation- Based Cooperation Enforcement in Ad Hoc Networks,‖ Technical Report, Stanford Univ., Standford, 2003.

[13] R. Akbani and T. Korkmaz, ―Enhancing Role-Based Trust Management with a Reputation System for MANETs,‖ URASIP Journal on Wireless Communications and Net- working 2011, 2011, p. 90.

[14] F. Wang. F. R. Wang, B. X. Huang and L. T. Yang, ―COSR: A Reputation-Based Secure Route Protocol in MANET,‖ EURASIP Journal on Wireless Communica- tions and Networking—Special Issue on Multimedia Communications over Next Generation Wireless Net - works Archive, Vol. 2010, 2010, pp. 1-11.

[15] S. R. Zakhary and M. Radenkovic, ―Reputation Based Security Protocol for MANETs in Highly Mobile Dis-connection- Prone Environments,‖ International Confer- ence on Wireless On- demand Network Systems and Ser- vices (WONS), 2010, pp. 161-167.

[16] Dr.G.Padmavathi , Dr.P.Subashini , and Ms.D.Devi Aruna ZRP with WTLS Key Management Technique to Secure Transport and Network Layers in Mobile Adhoc Networks International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, February2012