Various Security Attacks and Trust Based Security Architecture for MANET

Ankit Jain[1], Arnika Jain[2], Pramod Kumar Sagar[3]

GJCST Classification
C.2.0

***Abstract*-A Mobile Ad hoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets to each other allowing them to communicate beyond direct wireless transmission range. Mobile Ad hoc Networks (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. Security is an important issue for all kinds of networks including the Wireless Ad Hoc Networks. In this paper, we are presenting some of the reasons that have made MANETs more vulnerable to attacks than the traditional wired network. This paper also covers the security attributes and the various challenges to security design. This paper shreds light on some of the security attacks that exists in MANETs. This Paper also proposes Trust Based Security Architecture for MANET.**

*Index Term-s*Blackhole attacks, DoS and Flooding, Eavesdropping, Grayhole attacks, Impersonation, MANETs (Mobile Ad hoc Networks), Rushing, Wormhole attacks

I. Introduction

MANET is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed and can work at any place without the help of any infrastructure. The system may operate in isolation, or may have gateways to interface with a fixed network. This property makes MANET highly robust. The characteristics of these networks are summarized below:

- Autonomous and Infrastructure-less
- Dynamic Network Topology
- Self-organization and Self-administration
- No Centralized controller and Infrastructure: Intrinsic Mutual Trust
- Device Heterogeneity
- Bandwidth-Constrained
- Energy-Constrained Operation
- Multi-hop Routing
- Network Scalability
- Nodes can be both host or router
- Frequent Routing updates
- Limited Physical Security

About[1]- Technical Leader Software Development Department IBM India; SRM University ankitjain@in.ibm.com
About[2]- Assistant Professor CSE Department NCR Campus, Modinagar , jain.arnika2009@gmail.com
About[3]- Assistant Professor IT Department Ghaziabad (UP), India pksagar75@rediffmail.com

II. Security Problems In Manet

Security is one of the important issues for wired networks as well as for Wireless Ad Hoc Networks. MANETs are much more vulnerable to attacks than the wired networks due to system constraints in mobile devices which include low-power, open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and low battery power. The unique characteristics of MANETs present a new set of nontrivial challenges to security design which includes open network architecture, shared wireless medium, stringent resource constraints, highly dynamic network topology and some more. Some of the important ones are discussed below:

1) ***Open Medium:*** Eavesdropping is much easier in wireless networks than in wired networks.
2) ***Dynamically changing Network Topology:*** Mobile nodes come and go from network thereby allowing any malicious node to join the network without being detected.
3) ***Cooperative Algorithms:*** The routing algorithm of MANET requires mutual trust between nodes which violates the principle of network security.
4) ***Lack of Centralized Monitoring:*** Absence of any Centralized Infrastructure prohibits any monitoring agents in the system.
5) ***Lack of Clear Line of Defense:*** The line of Defense i.e. prevention, Detection and Response are needed. Security research in wired networks needs to deploy layered security mechanism because security is a process that is as secure as its weakest link.

III. Security Attributes

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment and the ultimate goal of the security solutions for MANETs is to provide security services such as Confidentiality, Integrity, Availability, Non-Repudiation and Authentication, Authorization and Anonymity.

1) ***Confidentiality*** ensures that Secret information or data is never disclosed to unauthorized devices.
2) ***Integrity*** tells that a received message is not corrupted.
3) ***Availability*** permits the survivability of network services despite Denial-of-Service attacks.

4) ***Non-repudiation*** ensures that the sender of a message cannot deny having sent the message.
5) ***Authentication*** enables a node to ensure the identity of the Peer node it is communicating with.
6) ***Authorization*** is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

Anonymity ensures that the information used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the System Software.

IV. Security Challenges

1) ***Channel Vulnerability:*** Broadcast Wireless channels allow message Eavesdropping and Injection easily.
2) ***Node Vulnerability:*** Nodes do not reside in physically protected places, thus easily fall under attack.
3) ***Absence of Infrastructure:*** Certification/ Authentication Authorities are absent.
4) ***Dynamically Changing Network Topology*** puts security of routing protocols under threat.
5) ***Power and Computational Limitations*** prevent the use of complex Encryption Algorithms.

V. Security Attacks

MANETs vulnerabilities and lacks give rise to attacks at network layer of ISO/OSI stack. There are basically two types of attacks: Active and Passive. In an active attack, information is inserted to the network and thus the network operation or some nodes may be harmed. Examples are Impersonation, Modification, Fabrication and Disclosure attack. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious. In a passive attack, a malicious node either ignores operations supposed to be accomplished by it (examples: silent discard, partial routing information hiding), or listens to the channel, attempting to retrieve valuable information (example: vesdropping). Nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this paper, we are discussing some of the active attacks given below:

1) *Impersonation*

An Act whereby one Entity assumes the identity and privileges of another Entity without restrictions and without any indication visible to the recipients of the impersonator's calls that delicately has taken place as shown in Fig 5.1.

2) *Blackhole attacks:*

A Blackhole is a malicious node that falsely replies for route requests without having an active route to the destination and exploits the Routing Protocol to advertise itself as having a good and valid path to a destination node. As shown in Fig 5.2, a malicious node tries to become an element of an active route, if there is a chance and it has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process.

3) *Grayhole attacks:*

A Grayhole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes as shown in Fig 5.3. In this type of attack, node may behave maliciously for some time but later on it behaves absolutely normally. This type of attacks is more difficult compared to black hole attack.

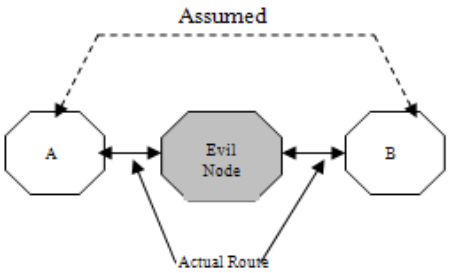

Fig 5.1 Impersonation

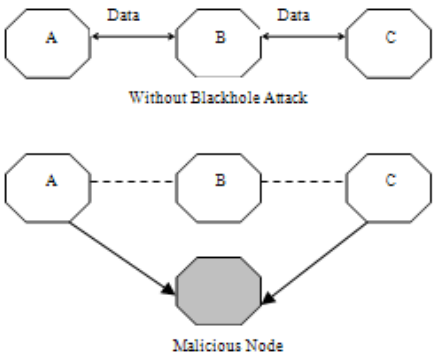

Fig 5.2 Blackhole Attack

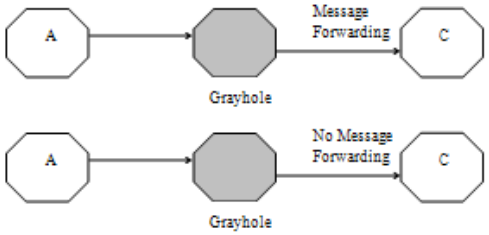

Fig 5.3 Grayhole Attack

4) *Wormhole attacks*

In a wormhole attack, a malicious node can record packets (or bits) at one location in the network and tunnel them to another location through a private network shared with a colluding malicious node. Wormhole attack can be done with one node also, but generally two or more attackers connect via a link called wormhole link. Wormhole attack is of three types: Closed Wormhole, Half Open Wormhole,

and Open Wormhole. All of these have been shown in Fig 5.4.

5) *Rushing*

When a neighbor of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard these legitimate REQUESTs as shown in Fig 5.5.

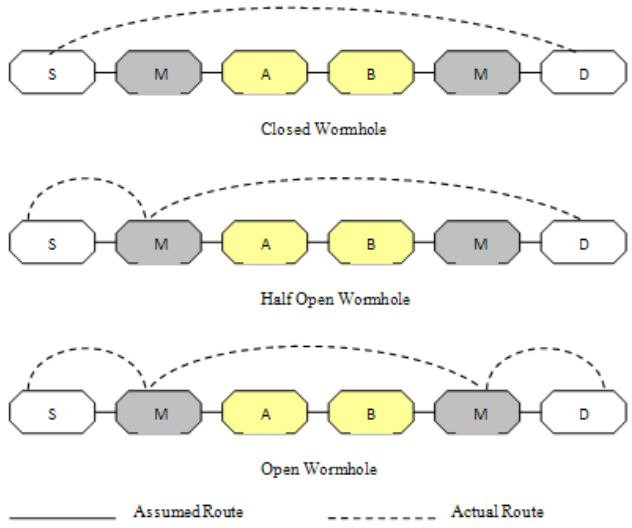

Fig 5.4 Wormhole

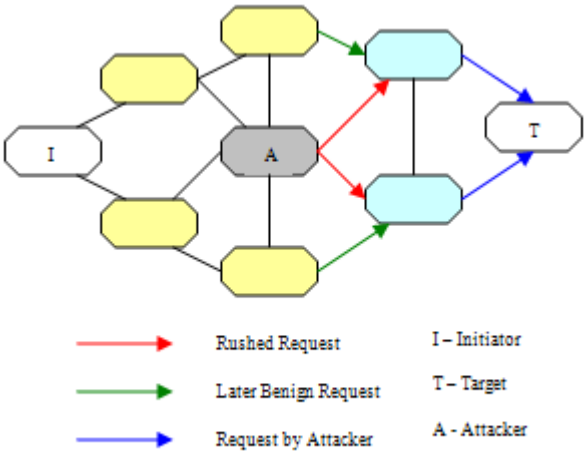

Fig 5.5 Rushing

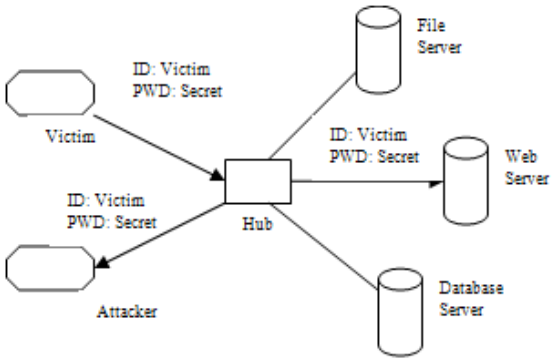

Fig 5.6 Eavesdropping

6) *Eavesdropping*

Eavesdropping is another kind of attack that usually happens in the Mobile Ad hoc Networks and is shown in Fig 5.6. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. This confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, it should be kept away from unauthorized access.

7) *DoS and Flooding*

In a Denial-of-Service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting client computer and its network connection, or the computers and network of the sites client is trying to use, an attacker may be able to prevent the client from accessing email, websites, online accounts, or other services that rely on the affected computer. The most common and obvious type of DoS attack occurs when an attacker floods a network with information as shown in Fig 5.7. When client types a URL for a particular website into browser, the server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process the legitimate request.

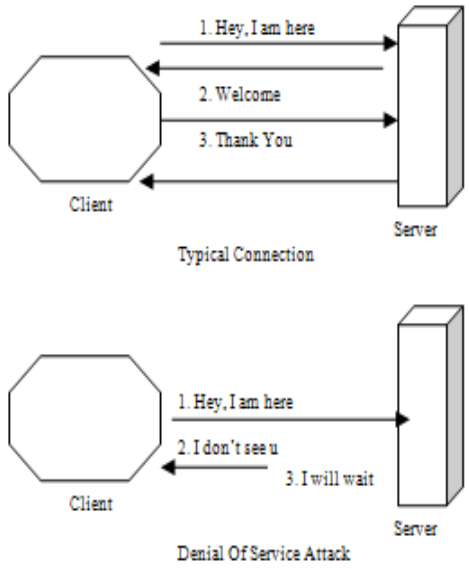

Fig 5.7 Denial Of Service Attack

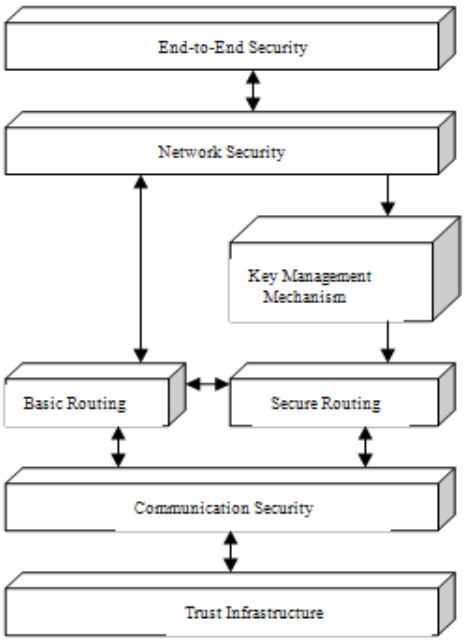

Fig 6.1 Trust Based Security Architecture

VI. Trust Based Security Architecture For Manet

Since in MANETs, there is no centralized authority for trust relationship between the nodes to communicate, this Paper proposes a Security Architecture for the secure transmission of data between MANET nodes named Trust Based Security Architecture for MANET. The objective of the architecture presented in this paper is to provide security in a Collaborative, Self-organized manner. It provides tolerance to compromised nodes, have the ability to detect and remove adversaries from network and handle routing misbehaviors. The model defined in our architecture differs from related models [1] and [2, 3] by defending against both Flooding and Packet drop attacks as is shown in fig 6.1.The Trust Infrastructure module corresponds to the trust relationship between nodes to communicate and it has various security mechanisms that are constructed in a distributed manner and are the basic building blocks of the entire security system. Communications Security module refers to the secure transmission of data from one node to another.Since Routing is an important part for a network so every node should participate in routing activity and thus leads to network topology so that the data packets can be routed to the correct destination. Routing Security refers to security corresponding to Routing Protocols. The Routing Security is categorized into two parts: Secure Routing and Secure data forwarding. In Secure Routing, a node cooperate to have correct routing information and thus keeps the network connected efficiently and in Secure Data Forwarding, data packets, while on the route, should be protected from tampering, dropping, and altering by any unauthorized party.The secure routing protocol is responsible to discover secure paths and to have secure data transmission through the secret associations established and maintained by the key management mechanism.

In this architecture, the Secure Routing Protocol forwards evidence for fabrication and modification attacks to the Trust Infrastructure module, and takes advantage of the Trust Infrastructure module feedback to make better routing decisions. Although the Key Management Mechanism [8] does not forward any evidence to Trust Infrastructure module, it relies heavily on its feedback to dynamically manage the keys. Network Security refers to the security mechanisms used by the network protocols which perform sub-network access operations from end system to end system. Secure Message Transmission [3] working at network security is a good example of security efforts done in the end systems as a remedy for the unreliable routing protocol. End-to-End Security refers to end system security. The security protocols at this level is independent of the underlying networking technology since the related security mechanisms are restricted to only intended parties. In sequence, this model is used to defend against both flooding and packet drop attacks.

VII. Conclusion

MANETs require a reliable, efficient, scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. In this paper, we discussed the vulnerable nature of the mobile ad hoc network, and owe to that; there are numerous security threats that disturb the development of it. This paper also covers the security attributes and the various challenges to security design. This paper also presents the security issues. Then it presents the main attack types that exist in it. This Paper has focused on designing security architecture in tackling security challenges that mobile ad hoc networks are facing. In this paper, we have proposed Trust Based Security Architecture for MANETs. We expect

this security architecture can be used as a framework when designing system security for ad hoc networks.

VIII. References

1) Balakrishnan, V. Varadharajan, U. K. Tupakula, and P.Lucs, *"Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks"*. Proceedings of 4th IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, 2007.
2) L. Buttyan and J. Hubaux, *"Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Ad hoc Networks"*. Technical Report (DSC/2001/001), Swiss Federal Institute of Technology, 2001.
3) P. Papadimitratos, Z. Haas, *Secure Data Transmission in Mobile Ad Hoc Networks*, ACM Workshop on Wireless Security, 2003.
4) M.S. Corson, J.P. Maker, and J.H. Cernicione, *Internet-based Mobile Ad Hoc Networking*, IEEE Internet Computing, pages 63–70, July-August 1999.
5) Lidong Zhou and Zygmunt J. Hass, *Securing Ad Hoc Networks*, IEEE Networks Special Issue on Network Security, November/December 1999.
6) Balakrishnan, and V. Varadharajan, *"Fellowship in Mobile Ad hoc Networks"*. Proceedings of 1st IEEE International Conference on Security and Privacy for Emerging Areas in communications Networks (SecureComm 2005), Athens, Greece, pp. 225-227, 2005
7) F. Stajano and R. Anderson: *The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless networks*. In Proceedings of the 7th International Workshop on Security Protocols, 1999.
8) S. Capkun, L. Buttyan, J. Hubaux: *Self-Organized Public-Key Management for Mobile Ad Hoc Networks*, IEEE Transactions on Mobile Computing, VOL.1, NO.1, 2002.
9) W. Lou, W. Liu, Y. Fang: *SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks*, IEEE INFOCOM, 2004.
10) H. Yang, X. Meng and S. Lu: *Self-Organized Network-Layer Security in Mobile Ad Hoc Networks*, ACM, 2002.