Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.792 – 800

RESEARCH ARTICLE

A STUDY OF ROUTING PROTOCOLS AND ATTACK PATTERNS ON ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS

Miss. S.Jothilakshmi[1], Mrs. R.Kavitha[2]

[1]M.Phil Research Scholar, Department Of Computer Science, Vivekanandha College for Women, Namakkal (India)

[2]Assistant Professor, Department Of Computer Science, Vivekanandha College for Women, Tiruchengode, Namakkal (India)

[1] clickjothi76@gmail.com, [2] kavithamscmphil@gmail.com

ABSTRACT: A Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions .This paper provides an study of different routing protocols. This paper presents some of the available secure routing protocols and most common attack patterns against ad hoc networks. Routing protocols are subjected to case studies against the most commonly identified attack patterns such as: denial-of-service attack, tunneling, spoofing, black hole attack and wormhole attack.

Keywords - MANETs, Routing Protocol, Security Issues

I. INTRODUCTION

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Ad Hoc networks do not have a certain topology or a central coordination point. Therefore, sending and receiving packets are more complicated than infrastructure networks.

Nowadays, with the immense growth in wireless network applications like handheld computers, PDAs and cell phones, researchers are encouraged to improve the network services and performance. One of the challenging design issues in wireless Ad Hoc networks is supporting mobility in Mobile Ad Hoc Networks (MANETs). The mobility of nodes in MANETs increases the complexity of the routing protocols and the degree of connection‟s flexibility. However, the flexibility of allowing nodes to join, leave, and transfer data to the network pose security challenges.

A MANET is a collection of mobile nodes sharing a wireless channel without any centralized control or established communication backbone. MANET has dynamic topology and each mobile node has limited resources such as battery, processing power and on-board memory. This kind of infrastructure-less network is very useful in situation in which ordinary wired networks is not feasible like battlefields, natural disasters etc. The nodes which are in the transmission range of each other communicate directly otherwise communication is done through intermediate nodes which are willing to forward packet hence these networks are also called as multi-hop networks.

Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), omnidirectional (broad-cast), probably steerable, or some combination.

II. REVIEW OF ROUTING PROTOCOLS

In MANETs, some form of routing protocol is required in order to dynamically detect the multi-hop paths through which packets can be sent from one node to another.

There are basically two categories of routing protocols for MANETs:

2.1. Table Driven (Proactive): DSDV, GSR, WRP

2.2. Source Initiated On-Demand (Reactive): ABR, AODV, DSR, LAR.

2.3. Hybrid routing protocols: ZRP, SHARP

2.1. Proactive or Table-Driven Routing Protocols

In table driver routing protocols, every node maintains the network topology information, in the form of routing tables by periodically exchanging routing information.Routing information is generally flooded in the whole network. Whenever a node requires a path to adestination, it runs an appropriate path finding algorithm on the topology information it maintains.

2.1.1. Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV is developed on the basis of Bellman–Ford routing algorithm with some modifications. In this routing protocol, each mobile node in the network keeps a routing table. Each of the routing table contains the list of all available destinations and the number of hops to each. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. So the routing information updates might either be periodic or event driven.

DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbors. The advertisement is done either by broadcasting or by multicasting. By the advertisements, the neighboring nodes can know about any change that has occurred in the network due to the movements of nodes. The routing updates could be sent in two ways: one is called a full dump and another is incremental. In case of full dump, the entire routing table is sent to the neighbors, where as in case of incremental update, only the entries that require changes are sent.

2.1.2. Wireless Routing Protocol (WRP)

WRP belongs to the general class of path-finding algorithms defined as the set of distributed shortest path algorithms that calculate the paths using information regarding the length and second-to-last hop of the shortest path to each destination. WRP reduces the number of cases in which a temporary routing loop can occur. For the purpose of routing, each node maintains four things: 1. A distance table 2. A routing table 3.A link-cost table 4. A message retransmission list (MRL).

WRP uses periodic update message transmissions to the neighbors of a node. The nodes in the response list of update message (which is formed using MRL) should send acknowledgments. If there is no change from the last update, the nodes in the response list should send an idle Hello message to ensure connectivity. A node can decide whether to update its routing table after receiving an update message from a neighbor and always it looks for a better path using the new information. If a node gets a better path, it relays back that information to the original nodes so that they can update their tables. After receiving the acknowledgment, the original node updates its MRL. Thus, each time the consistency of the routing information is checked by each node in this protocol, which helps to eliminate routing loops and always tries to find out the best solution for routing in the network.

2.2. Reactive or On-Demand Routing Protocol

Protocols that fall under this category do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routine information periodically.

2.2.1. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a reactive protocol based on the source route approach. In Dynamic Source Routing (DSR) protocol is based on the link state algorithm in which source initiates route discovery on demand basis. The sender determines the route from source to destination and it includes the address of intermediate nodes to the route record in the packet. DSR was designed for multi hop networks for small Diameters. It is a beaconless protocol in which no HELLO messages are exchanged between nodes to notify them of their neighbours in the network.

2.2.2. Ad Hoc on-Demand Distance Vector Routing (AODV)

AODV is basically an improvement of DSDV. But, AODV is a reactive routing protocol instead of proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded.

The reply is sent using the reverse path.For route maintenance, when a source node moves, it can reinitiate a route discovery process. If any intermediate node moves within a particular route, the neighbor of the drifted node can detect the link failure and sends a link failure notification to its upstream neighbor. This process continues until the failure notification reaches the source node. Based on the received information, the source might decide to re-initiate the route discovery phase.

2.2.3. Associativity-Based Routing (ABR)

ABR protocol defines a new type of routing metric “degree of association stability” for mobile ad hoc networks. In this routing protocol, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates beacon to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity table. For each beacon received, the associativity tick of the receiving node with the beaconing node is increased. A high value of associativity tick for any particular beaconing node means that the node is relatively static. Associativity tick is reset when any neighboring node moves out of the neighborhood of any other node.

2.3. Hybrid Routing Protocols

Protocols belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned or within a particular geographical region are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes that are located in this zone, are on-demand approach is used.

2.3.1. Zone Routing Protocol (ZRP)

ZRP is suitable for wide variety of MANETs, especially for the networks with large span and diverse mobility patterns. In this protocol, each node proactively maintains routes within a local region, which is termed as routing zone. Route creation is done using a query-reply mechanism. For creating different zones in the network, a node first has to know who its neighbors are. A neighbor is defined as a node with whom direct communication can be established, and that is, within one hop transmission range of a node.Neighbor discovery information is used as a basis for Intra-zone Routing Protocol (IARP). Rather than blind broadcasting, ZRP uses a query control mechanism to reduce route query traffic by directing query messages outward from the query source and away from covered routing zones. A covered node is a node which belongs to the routing zone of a node that has received a route query.

During the forwarding of the query packet, a node identifies whether it is coming from its neighbor or not. If yes, then it marks all of its known neighboring nodes in its same zone as covered. The query is thus relayed till it reaches the destination. The destination in turn sends back a reply message via the reverse path and creates the route.

2.3.2. Sharp Hybrid Adaptive Routing Protocol (SHARP)

SHARP adapts between reactive and proactive routing by dynamically varying the amount of routing information shared proactively. This protocol defines the proactive zones around some nodes. The number of nodes in a particular proactive zone is determined by the node-specific zone radius. All nodes within the zone radius of a particular node become the member of that particular proactive zone for that node. If for a given destination a node is not present within a particular proactive zone, reactive routing mechanism (query-reply) is used to establish the route to that node.

Proactive routing mechanism is used within the proactive zone. Nodes within the proactive zone maintain routes proactively only with respect to the central node. In this protocol, proactive zones are created automatically if some destinations are frequently addressed or sought within the network. The proactive zones act as collectors of packets, which forward the packets efficiently to the destination, once the packets reach any node at the zone vicinity.

III. CASE STUDIES OF ATTACK PATTERNS ON ROUTING PROTOCOLS

There are quite a number of routing protocols that are excellent in terms of efficiency. But the security requirements of these protocols changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To address these concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD), Ariadne, and Authenticated Routing for Ad hoc Networks (ARAN), Secure Ad hoc On-Demand Distance Vector Routing (SAODV), and Secure Routing Protocol (SRP).

3.1. Secure Efficient Ad hoc Distance Vector (SEAD)

SEAD was developed based on Destination Sequence Distance Vector (DSDV) and incorporates One-Way Hash function to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. An attacker cannot create a valid route with a larger sequence number that it received due to the properties of hash function. As SEAD incorporates neighbor authentication through Hash functions, an attacker can not compromise any node. SEAD is prone through wormhole attack. Even if authentication is provided using hash functions, a wormhole attack is possible through tunneling the packets from one location and retransmitting them from other location into the network.

All packets in the wormhole attack flow in a circle around instead of reaching the destination. Routing table overflow attacks are possible in SEAD, as SEAD is developed based on a table driven approach. A compromised node can advertise routes to nodes which are not in the network and there by fill in the space allocated in the routing table with false node routes. Spoofing attack is possible through compromised node acting like a destination node in the route discovery process by spoofing the identity of the destination node that can cause route destruction. Black hole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Tunneling and DOS attacks are also possible through compromised nodes. Table driven protocols are much more prone to security threats.

3.2. Ariadne

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MACs and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. Wormhole attacks are possible in Ariadne through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

3.3. Secure Routing Protocol (SRP)

Secure routing protocol (SRP) was developed based on Destination Source Routing (DSR). The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbors and maintain a priority ranking inversely proportional to the query rate. So the malicious compromised nodes participating in the network are given least priority to deal with. The security analysis is similar to Ariadne as it is based on DSR protocol.

3.4. Authenticated Routing for Ad hoc Network (ARAN)

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbor node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause congestion in the network, there by compromising the functionality of the network.

Spoofing attacks are prevented by ARAN through node level signatures. Each packet in the network is signed by its private key before broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN. Due to the strong cryptographic features of ARAN, malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern. Tunneling attacks are possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Wormhole attack is also possible through two compromised nodes. Table overflow, black hole attacks are impossible due to node level authentication with signatures.

3.5. Secure Ad hoc On-Demand Distance Vector Routing (SAODV)

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible replay attacks.

IV. CONCLUSION

In this paper a number of routing protocols for MANET, which are broadly categorized as proactive and reactive and Hybrid protocols. This paper discusses common possible attacks on different protocols being used in MANETs. We have tried to analyze them so as to prevent the attacker to intrude in wireless networks. There are lots of techniques with which, one can easily detect most of the attacks. One can choose them in accordance with the protocol being used in the network. However, no protocol is fully secure from attacks being encountered in the MANETs. Hence, one must choose a combination of techniques intelligently to avoid any attack and make the network fully secure.

REFERENCES

[1] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011.

[2] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2-17).

[3] Hao Yang, Haiyun Luo, Fan Ye, songwu Lu and Lixia Zhang,"Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications, Vol. 11, (2004) pp. 38-47.

[4] Hoang Lan Nguyen, Uyen Trang Nguyen "A study of different types of attacks on multicast in mobile ad hoc networks", Journal of Ad hoc Networks, Vol. 6, (2006),pp. 32-46.

[5] Sudhir Agarwal, Sanjeev Jain, sanjeev Sharma,"A survey of Routing attacks and security Measures in mibile adhoc networks", Journal of computing, Vol 3, Issue 1,(2011), pp. 41-48.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela cardei,"A survey on Attacks and Countermeasures in Mobile ad hoc networks", Wireless/Mobile network security, Springer,(2006).

[7] Manel Guerrero Zapata, N. Asokan in Nokia research center and was submitted to WiSe'02, September 28, 2002, Atlanta, Georgia, USA".

[8] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).

[9] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).

[10] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.

[11]Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang [2005]. "Resisting Flooding Attacks in Ad Hoc Networks". Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'05).

[12] Anand Patwardhan, Jim Parker and Anupam Joshi**.** "Secure Routing and Intrusion Detection in Ad Hoc Networks". [On-line] accessed on 6th November, 2005 at URL http://csrc.nist.gov/mobilesecurity/ Publications/ nist-umbc-adhocids-ipv6.pdf.

[13] Panagiotis Papadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.