ROUTING PROTOCOL AND SECURITY THREATS IN MANET

Ms V. Divya, Dr. R. Gobinath

Abstract— In wireless network MANET uses mobile nodes for transmitting data with external transmission range. Network results in multiple authentication problems that reduce the development of the network. In this paper the issues and attacks in mobile ad hoc network were fully categorized and analysed. External and Internal attacks are also analysed. Along with the security, the advanced routing techniques are also concentrated. This paper mainly focuses on security problems and the packet routing solutions in wireless MANET.

Index Terms— Pro-active protocol, Re-active protocol, Hybrid protocol, Blackhole and Worm hole attacks, cryptography.

1 INTRODUCTION

MANET is the ad hoc wireless network that includes routable network environment which uses multi hoping techniques to communicate. Each mobile node in the mobile networks forwards the data packet to neighbour nodes in the topology of the network. The nodes are designed without fixed infrastructure which allows them to move randomly as the topology of network changes. The nodes in the network are acting like the routers.

Each and every node in the MANET records the required information to route data traffic in proper manner. This is the main challenges in wireless ad hoc network.

2 MANET ATTACKS

2.1 Security Attacks

Providing security in MANET is a tedious process. Identify the type of attack in the network to provide solution for the security problem. Security attacks can be of two categories;

1) Internal Attack
2) External Attack

Internal Attack: Internal attack is the attack created from the nodes arranged in the wireless network. It is a type of attack in which the nodes get an unauthenticated access which acts as normal mobile nodes in the network topology.

External Attack: External attack is the security attack initiated by the nodes present outside the network topology. This type of attack produces wrong information about the routing service in the network. External attack is categorized as two classifications;

- Active attacks
- Passive attacks

- *Ms.V. Divya, Research Scholar, Department Of Computer Science, Vels Institute Of Science, Technology And Advanced Studies (VISTAS), Pallavaram, Chennai, Assistant Professor, Department Of Computer Science, Prince Shri Venkateshwara Arts And Science College Chennai. Email: divyavenkatraman1992@gmail.com*
- *Dr. R. Gobinath, Associate Professor, Department Of Computer Science, VISTAS, Pallavaram, Chennai.*

Active attack: The active attacks are either internal or external attack. This type of attack changes the resource and operation of the system. The active attack modifies the data stream during data transmission which results in wrong statement creation. This attack is very difficult to detect and very harmful. Active attack is created by the attacker mobile node in the structure of network, which suggests the wrong route link as the best communication route.

Passive attack: It is the attack which does not change the data stream during the data transmission. Network traffic is monitored in the passive attacks. The network routing protocols are not altered instead its information's are tracked and monitored. Strong Cryptographic algorithms are used for avoiding this type of attacks.

Worm hole attack: It is the type of harmful security attacks. In worm hole attack, a tunnel is made in between the two attacker node in the network by the hacker. The tunnel between the nodes is denoted as a worm hole. This type of attacks undergoes without revealing the identities of unauthorized person.

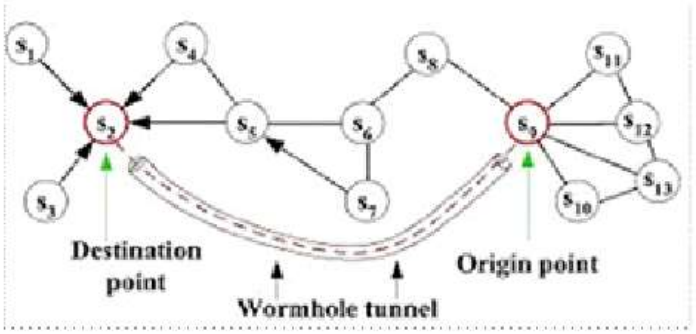

Figure 1-Wormhole attack in routing [1]

Blackhole attack: The node is said to be a blackhole, if it response RREP packet for every RREQ packet through the wrong route to the destination. This type of nodes does not verify the routing information. In case of blackhole attack, a packet transmitted by the source were not forwarded to the destination instead it is dropped by the black hole node. The blackhole attack will divert the route in the structure of network which causes network traffic.

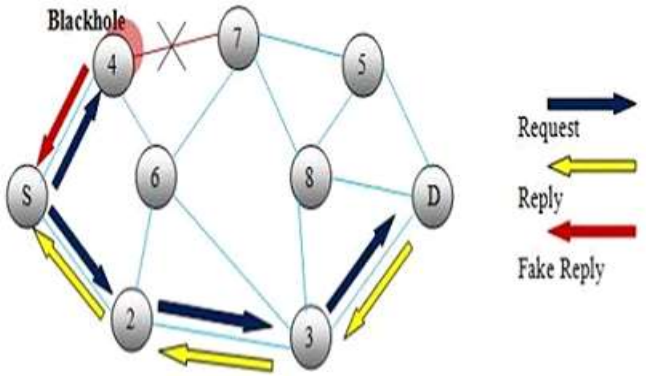

Figure 1-Black hole attack in MANET [2]

2.2 MANET PROTOCOLS FOR ROUTING

A most helpful tool to understand the operation of wireless network is the Networks Simulator (NS). A protocol features included in the mobile network is;

- Adopting modification in the topology of the network.
- Providing multiple routes between the sender and receiver.
- Minimal control messages.
- Quick route establishment.

Protocols for routing used by the wired and mobile networks are categorized into four types depending on their attributes. They are;

i. Centralized and Distributed
ii. Static and Dynamic
iii. Flat and Hierarchical
iv. Proactive, Reactive and Hybrid

Centralized and Distributed: In the centralized routing, the routing decision is made at the middle node in the network. The entire details about the network topology are maintained by the centralized node. In case of distributed routing the detail is shared between the nodes and the routing decision about the packet is made.

Static and Adaptive: The static routing provides more security to the network during data transmission. Unless the network operator changes the routing table manually, the table information is not modified in static routing. The other name for adaptive routing is termed as dynamic routing. In dynamic routing the routing tables are modified as the network topology changes. It does not provide more security like static routing and uses complex routing algorithms.

Flat and Hierarchical: Each and every node in the flat routing are represented as peers. The detail about the routing is distributed to the entire nodes in the environment that are connected to the routers. In hierarchical routing, unlike flat routing each and every node in the network is treated with individual responsibility. In the hierarchical routing, the network is classified as clusters where each node performs specific task.

Proactive routing: Routing information about the network is updated using proactive routing. Table driven protocol represents the table in which the routing information is maintained. In proactive routing, every node contains single or multiple routing tables that are recorded at regular manner. To determine the changes in the structure of network, the routing detail is transferred to the entire node in the topology. The advantages of proactive routing are as follows;

- Provides actual information.
- Network availability is increased

The disadvantages of proactive routing are;

- Maintenance cost is over headed.
- Results with fewer throughputs

Re-active routing: The structure of the network was determined using reactive protocol. In re-active routing, the path is discovered in advance by every node in the environment. Once a route is discovered, a control message is flooded in order to discover the on demand route. The nodes in the network do not maintain the continuous route between them. The routes are established by the nodes at the time of requirement. The advantages of reactive routing are as follows;

- No periodic update of routing table.
- Routing overhead is reduced.

The disadvantages of proactive routing are;

- High latency.
- Less storage capacity.

Hybrid routing: Pro-active protocol and re-active protocols are combined together and termed as hybrid routing protocol. In hybrid protocol, the mobile nodes are divided into zones. Pro-active routing is utilized in each zones of the route and re-active routing is used between the routing zones. The disadvantages of proactive routing are;

- Designed for large network.
- Less overhead
- Low latency.

The main disadvantage of hybrid routing is very difficult to implement.

2.3 SECURITY FOR ROUTING IN MANET

MANET undergoes more vulnerability due to the reduction of authority. Therefore the authentication process is the important requirements in wireless network. AODV protocol has no security measures in it.

Ad-hoc on demand distance vector (AODV) protocol for routing:

AODV is the re-active type routing, where the path discovery process is made in advance. It creates the path between sender and receiver node when it is required. To communicate the data with other nodes, the routes are built by certain nodes, only after sending the route discovery message. The information about the route is recorded only in sender node, receiver node and in the intermediate node. AODV communication undergoes three main procedures;

1. Route discovery
2. Route establishment
3. Route maintenance

The messages used in AODV implementation are as follows;

1. Request Message (RREQ)
2. Route Reply (RREP)
3. Route Error (RERR)

The RouteREQuest and RouteREPly packet formats are shown below:

RREQ Packet Format

Source Address	Source seq	Broadcast ID	Destination Address	Destination seq	Hop count

RREP Packet Format

Source Address	Destination Address	Destination seq	Hop count	Lifetime

Path Discovery: Route discovery process in AODV protocol is entirely on advance. The sender node sends the RouteREQuest packet to its neighboring node when there are no path between the sender and receiver to transmit a packet. Each and every node contains the sequential number to avoid loops in routing. The sequential number of the receiver is included in the RouteREQuest message. When the intermediate node receives the RouteREQuest message, it first verifies its own sequential number in the route table entry. If the sequential number of the intermediate node is greater than sequential number associated with RREQ message, then the intermediate node forward the RREP packet back to the neighbor which transferred RREQ message to it. In this way the fresh route is supplied between the sender and receiver with the help of intermediate nodes.

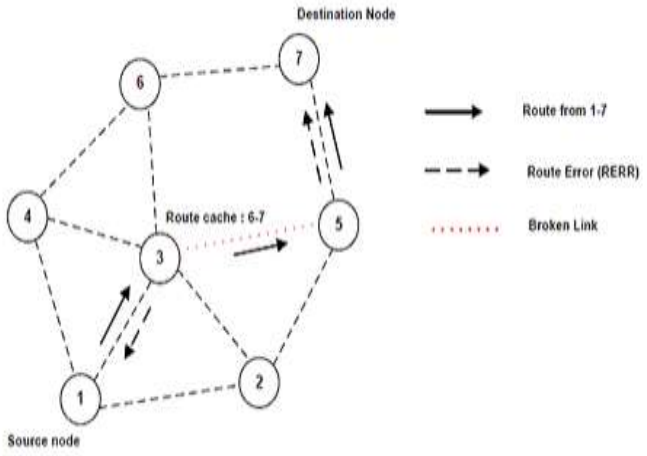

Figure 2- Path discovering process in AODV routing [3]

Path maintenance: To handle the dynamics in the topology of the network, route maintenance technique is used. Route maintenance is used to monitor the link breakage between the active nodes. An unsolicited RREQ message with fresh sequence number is send to all the active nodes as soon as the link is broken.

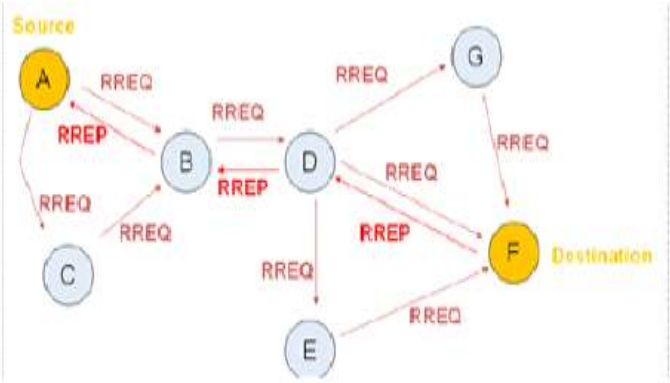

Figure 3-Route maintenance in AODV protocol [4]

AODV routing with Twofish cryptography

AODV protocol has no security measures in it. Therefore twofish cryptographic technique is used with AODV (MAODV) to treat the security issues in AODV protocol. The work is simulated using Network Simulator (NS2) with different number of malicious nodes and pause time. Two fish cryptographic algorithm is a symmetric block cipher. This technique uses single key for both encryption and description. It supports 128 bits of block cipher. The maximum length of the key is up to 256 bits. This cryptography undergoes 16 rounds of authentication. At each round two 32 bit word segment of the text block acts as an input to the to the F function. The twofish cryptography consists of 4 key dependent S-boxes, as each word in the first round is broken into 4 bytes. Twofish cryptography is the Fiestel type of network. In each round of the algorithm, two 32 bit word segment of the text block act as input to the F function. Each word further divided into 4 bytes. Therefore 4 key dependent S – Boxes are used to send these 4 bytes.

The twofish cryptography algorithm is very strong and simple. The round function at each step is said to bijective (all the outputs are possible). This technique includes many mathematical and algebraic operation groups such as s-box substitution, MDS matrix, XOR-addition, PHT which makes the attack very difficult while transmitting the packet through the network. The algorithm also prevents related key attacks.

S – Box: It is the substitution box implemented as the lookup table. It is one of the major elements of symmetric key technique used for performing a substitution operation. This component identifies the relationship between the key and cipher text (confusion property). S-box contains m-input bits and n-output bits (m-input x n-output s-box). It is denoted as the lookup table with 2m words. Each word contains n bits.

MDS matrix: The Maximum Distance Separable matrix is the matrix function with diffusion property used for hiding the relationship between the plaintext and cipher text with the help of cryptographic hash function. This component is used to protect the block cipher against the attack.

PHT: The Pseudo Hadamard Transform is a bit transformation which provides the diffusion property. This component divides the even length bit string into two equal length string namely a and b. The transformation can be denoted as;

$$b= b'-a' \ (mod\ 2^n)$$

$$a=2a'-b' \ (mod\ 2^n)$$

3 CONCLUSION

For developing the mobile network, security is the most significant aspects. To mitigate a effects of security issues in AODV re-active protocol, it is imperative to implement an effective cryptographic technique in AODV protocol. This paper propose an effective twofish cryptographic technique in AODV [MAODV] protocol to provide authentication against attacks due to route breakage in existing AODV routing protocol, which establish the secured route path for data communication over wireless network. The speed, flexibility and design of twofish cryptography is also analyzed in this paper, which proves that twofish cryptography is the best technique of all the AES cryptography.

REFERENCES

[1] Iqbal, Muddesar & Shafiq, Muhammad & Choi, Jin-Ghoo & Attaullah, Hasina & Akram, Khawar & Wang, Xingheng. (2014). Design and Analysis of a Novel Hybrid Wireless Mesh Network Routing Protocol. International Journal of Adaptive, Resilient and Autonomic Systems. 5. 20-39. 10.4018/ijaras.2014070102.

[2] Study of Security Attacks In MANET 11BCE111 KUNAL PRAJAPATI.

[3] The Internet-of-Things (IoT) Security : A Technological Perspective and Review, Dr. Yusuf Perwej et al Int J Sci Res CSE & IT. January-February-2019; 5(1): 462-482.

[4] Route maintenance in www.rroij.com

[5] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu, “Risk-Aware Mitigation for MANET Routing Attacks”, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, pp. 250-260, 2012.

[6] Priyanka Goyal, Viniti Parmar and Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, International Journal of Computational Engineering & Management, Vol. 11, pp. 32-37, 2011.

[7] Neetu Singh Chouhan and Shweta Yadav “Flooding Attacks Prevention in MANET”, International Journal of Computer Technology and Electronics Engineering, Vol. 1, No. 3, pp. 68-72, 2011.

[8] Gagandeep, Aashima and Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”, International Journal of Engineering and Advanced Technology, Vol. 1, No. 5, pp. 269-275, 2012.

[9] Amrit Suman, Praneet Saurabh and Bhupendra Verma, “A B.ehavioral Study of Wormhole Attack in Routing for MANET”, International Journal of Computer Applications, Vol. 26, No. 10, pp. 42-46, 2011.

[10] Ammar Odeh, Eman AbdelFattah and Muneer Alshowkan, “Performance evaluation of AODV and DSR routing protocols in MANET Networks”, International Journal of Distributed and Parallel Systems, Vol. 3, No. 4, pp. 13-22, 2012.

[11] Punardeep Singh, Harpal Kaur and Satinder Pal Ahuja, “Brief Description of Routing Protocols in MANETS And Performance And Analysis (AODV, AOMDV, TORA)”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 1, 2012.

[12] Anju Gill and Chander Diwaker, “Comparative Analysis of Routing in MANET”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 7, 2012.

[13] Rajiv Chechi, Vikas Malik and Ompal Gupta, “Classification of Routing Protocols in MANET & their Pros & Cons: A Review”, International Journal of Research in IT & Management, Vol. 2, No. 11, pp. 28-31, 2012.

[14] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications, Vol. 2, No. 1, 2012.