AN EFFICIENT IDRS APPROACH TO ABOLISH THE ROUTING ATTACKS IN MANET.

Nivedha.E.
P.G Student ,Dept of IT.
Sri Sairam Engineering College,Chennai.
nivedhaelangovan24@gmail.com.

Usha.S
Associate Professor, Dept of IT.
Sri Sairam Engineering College. Chennai.
usha.it@sairam.edu.in

Abstract— A MANET is a category of wireless ad hoc network that can change locations and configure itself. These type of networks are without fixed infrastructure and are more prone to attacks that occur in the network. The existing methodologies namely 2ACK,NACK,SMP and STP results its inefficiency in detecting attacker's intrusion during collisions and have high routing overhead.In this paper we developed an efficient IDRS approach to purge the routing attacks in MANET. This was accomplished by the Reactive Routing protocol like DSR in MANET. An Extended Dempster shafer theory was used to detect the attacks and Cryptographic schemes like RSA,Certificate Distribution are used to isolate the attack from the network.A Simulation environment was created by Network Simulator-2.3.

Keywords-MANET, RSA, IDRS, Dempster shafer theory.

I. INTRODUCTION

A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers connected by wireless links.The routers are free to move randomly and organize themselves capriciously.Thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion. Due to a lack of infrastructure support, each node acts as a router, forwarding data packets for other nodes. The routing of data packets in a Mobile Ad hoc network is shown in figure1.

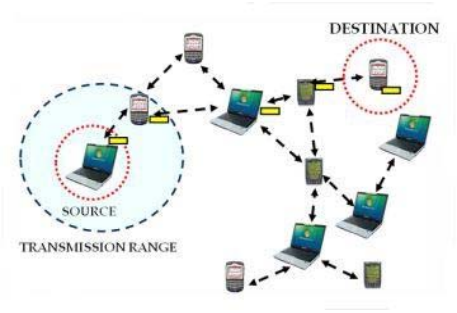


Figure 1 MANET Routing

In this paper we deal with different types of attacks which occurs in the network layer.The following paper is organized as follows.Section II describes several types of attacks in MANET. Section III describes Related work.Section IV deals with Proposed work and different Schemes to isolate the routing attacks in MANET.Section V concludes the work and gives the future scope.

II. ATTACKS IN MANET

There are different types of attacks in MANET which occurs in all the layers of the network.In Network layer the active and passive attacks are more important.The active attacks are discussed in this following paper.

A. Sleep Deprivation Attack.

This kind of attack is actually more specific to the mobile ad hoc networks. The motto is to sap

off restricted resources in the mobile ad hoc nodes (e.g. the battery powers), by unremittingly makes them busy processing unnecessary packets. In a routing protocol like DSR, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the network.

B. Link Spoofing Attack

In a link spoofing attack, an attacker node advertises fake links with non-neighbors to disrupt routing operations.For example, in the DSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the invalid path.

III. RELATED WORK

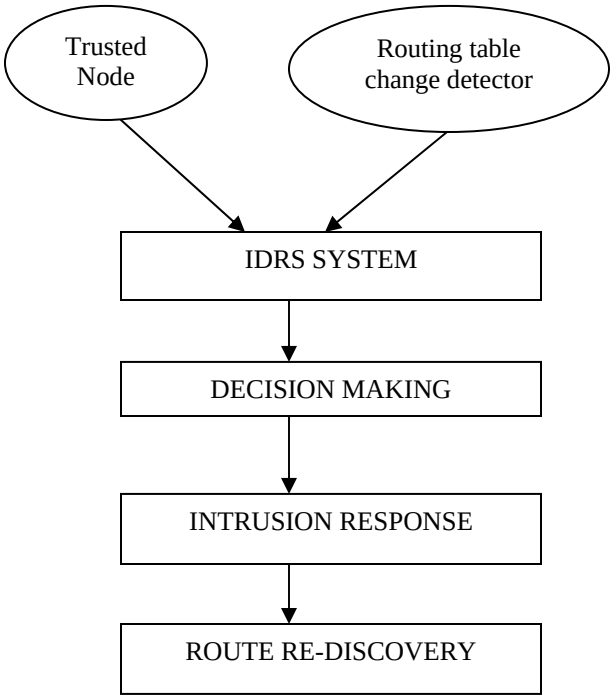
Some security related works has been proposed in MANET.An existing solution states that Reputation based security protocol is used in DSR to detect and remove malicious nodes.The key advantage of this protocol is that Black hole attack is detected easily and efficiently than AODV.Reference[2][3] gives an overview of the routing protocols such as ARAN, the known routing attacks and the proposed countermeasures to these attacks in various works. Reliability is increased through trusted certificates and digital signatures. In reference[4] new key management scheme is implemented in NTP protocol. Node Transition Probability (NTP) based algorithm provides maximum utilization of bandwidth during heavy traffic with less overhead. NTP determines stable routes using received power. This proposal detects the modification, impersonation attacks and TTL attacks and avoids the effects of malicious node and provides appropriate measures to discard such malicious nodes in dynamic condition. Reference[5] proposed a new model called EIDAN(Enhancement on Intrusion Detection System) makes use of Novel architecture to detect active attacks.This model is very efficient in detecting resource consumption attack,fabrication attack. Reference[7] states that two trust models have been proposed namely probability model and entropy model.The malicious misbehavior of nodes are characterized by these two models.The trust value is assigned to be one.A trust graph is generated which is used to differentiate malicious nodes and good nodes.The proposed theoretical models are then applied to improve the performance of ad hoc routing schemes. Reference[11] proposed an extension to the TWOACK scheme, in which each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This scheme requires an end to end Ack packet (i.e. Nack) to be sent between the source and the destination.

IV. IDRS APPROACH

The proposed work is to detach the routing attacks that takes place in the network layer of MANET. So an Adaptive IDRS approach is developed to perform the detection and avoidance of attacks in the network layer.Here IDRS stands for Evidence Collection, Assessment of Risk,Decision making and Risk Response.In the Evidence Collection phase the evidences are obtained from the trusted node and the routing table change detector. In the next step Assessment of riskee is detected by using Extended Dempster Shafer theory.It is used for risk assessment calculation.Then based on these values the adaptive decision making process takes place.The Risk response is done by cryptographic schemes.This approach is implemented in the following way. Initially a trusted node is created and that node acts as (IDS/IRS).Further occurrence of an

attack is confirmed and necessary measures are taken to detect, avoid and segregate the attacks.Then the route is re-established by using this Ondemand Dynamic Source Routing protocol. DSR is a Reactive routing protocol which possess two phases namely Route Construction and Route Maintenance phases.It establishes the route only when it is needed by the source or destination node.

A. SYSTEM FLOW



B. Solution to Link Spoofing Attack

The attacker node is detected and avoided in the following way. Initially the attacker node intentionally advertises the fake links to neighbor.The attacker node is detected based on criteriums like the Node which drop packets believing the fake links.

a) Avoidance

Step1: Initially source node broadcasts key to every node in the shortest path.

Step2: Then attacker node which drops packet is isolated from the network by using an Enhanced authentication protocol(EAP) Scheme.It then provides security,reliability and is the good scheme for authentication.

EAP Scheme involves these steps

1.Generation of nonce by both the server and client.

2.Generation of client ID,server ID takes place in both the server and client side .

3.Generation of master secret is done by using nonce, server ID in the server side.

4. Generation of master secret is done by using nonce, client ID in the client side.

5.Then the master secret is transmitted to server side and then authenticated by server side.

6. Successful data transmission with success message.

D. Solution to Sleep Deprivation Attack.

The attacker node is detected based on criterias like Nodes which excessively flood packets to neighbor node,Battery power – zero.

a) Avoidance

Step1:Initially Energy levels of all nodes in the shortest path are determined by the trusted node(source node).

Step2:Then the packet routing takes place in that path.The attacker node keep on flooding the packets and its energy level becomes zero(attacker node is drained off).

Step 3:Once the packet has been reached the destination node, it replies with the acknowledgement.Meanwhile the attacker node is drained off and its unable to reply to its neighbor.Within a TTL source node doesn’t get the ACK packet.

Step4:Then again the energy level is determined by source node and the attacker node is identified and isolated.

V. CONCLUSION

The attacks are the major Risks to MANET.These attacks are overcomed by many existing methods. In this paper we developed an efficient IDRS approach to detect and avoid the attacks in the network layer.Different Methods are provided in this paper which abolishes the routing attacks in MANET. The Schemes discussed above provides increase in throughput,security. and reliability.The Scope of future work is to provide solutions to different attacks in the network layer and to work on reducing routing overhead.

VI. REFERENCES

[1] Ziming Zhao, Gail-Joon Ahn March/April 2012 "Risk aware mitigation for MANET routing attacks" IEEE Transactions on Dependable and Secure computing, Vol. 9, no. 2

[2] Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang fourth quarter 2011 "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" IEEE Communications surveys & tutorials, vol. 13, no. 4,

[3]Noman Mohammed, Hadi Otrok, Lingyu Wang,Mourad Debbabi, and Prabir Bhattacharya January-February 2011 "Mechanism Design-Based Secure Leader Election Modelfor Intrusion Detection in MANET" IEEE transactions on dependable and secure computing, vol. 8, no. 1

[4] Andrzej K. Brodzik, and Robert H. Enders November 2011"Semigroup Structure of Singleton Dempster Shafer Evidence Accumulation"IEEE transactions on Information theory, vol. 55, no. 11

[5]B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A.Jamalipour, Oct. 2007 "A Survey of Routing Attacks in Mobile Ad hoc Networks," IEEE Wireless Communication Magazine, vol. 14, no. 5.

[6] Yan Lindsay Sun, Wei Yu, Zhu Han and K.J.Ray Liu , February 2006 "Information Theoretic Framework of Trust Modeling and Evaluation for Ad hoc Networks" IEEE journal on selected areas in communications, vol. 24, no. 2.

[7] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, May 2007 "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE transactions on mobile computing, vol. 6, no. 5.

[8] Q. He, D. Wu, and P. Khosla,2004, "SORI: A secure and objective reputation based incentive scheme for ad-hoc networks," in Proceedings IEEE Wireless Communication Network Conference., vol.2.

[9] G. Anastasi, M. Conti, E. Gregori, 2003,"IEEE 802.11 ad hoc networks: protocols, performance and open issues" IEEE Press Wiley.

[10] Y.C. Hu, A. Perrig, and D.B.Johnson, April 2003, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Network," Proc. 22nd Annual Joint Conf. IEEE Computer and Communication Societies San Francisco, CA.

[11] Amitabh Misgra and Ketan M. Nadkarni, ,2003, "Security in Wireless Ad hoc Networks", in Book The Handbook of Ad hoc Wireless Networks(Chapter 30),CRC Press LLC.

[12]S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp.576-578.