International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

AN ADAPTIVE EADR APPROACH TO PURGE THE ROUTING ATTACKS IN DSR

Nivedha.E[1], S.Usha[2]

[1] PG Student, M.E. Computer and Communication, Sri Sai Ram Engineering College,Chennai 44.
[2] Associate Professor, Department of IT, Sri Sai Ram Engineering College, Chennai 44.

nivedhaelangovan24@gmail.com, usha.it@sairam.edu.in

Abstract

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. These types of wireless networks are more prone to vulnerabilities.The pre-existing research efforts results its inefficiency in detecting attacker's intrusion during collisions and have high routing overhead.In this paper we propose an Adaptive EADR approach to defecate the routing attacks in Reactive Dynamic Source Routing Protocol.This was fostered by probabilistic Extended Dempster Shafer Theory of Importance factors.The robustness of our approach was shown in terms of our performance metrics.

***Keywords*-- MANET ,EADR, Dempster Shafer Theory**

I. INTRODUCTION

MANET is a type of wireless ad hoc network which has a self configuring capability. Every node acts as a mobile router with no access point. The unique features of MANET includes Multi-hop routing, Device heterogeneity,Bandwidth constrained variable capacity links, Limited physical security and Network scalability.The data transmission in MANET takes place by using multi-hop paths is shown in Figure 1

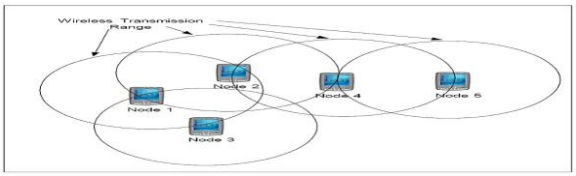

Fig 1 MANET Design

There are a wide variety of routing attacks that target the weakness of MANET. Of them Active and Passive attacks are more important.

Passive attacks: A passive attack is a one that does not interrupt the normal operation of the network. The attacker snoops the data exchanged in the network without altering it.

Active attacks: An active attack interrupts the regular operation of the network by destroying the data that are exchanged in the network. Active attacks can be internal or external. External attacks are done by nodes that do not belong to the network.

Internal attacks are launched by compromised nodes that are part of the network.In this paper we deal with the routing salvage attack which occurs in the network layer.

Routing Salvage Attack: The attack is launched by greedy internal nodes. Misbehaving nodes will fabricate and retransmit packets even though they haven't received error messages.This attack leads to unnecessary bandwidth consumption and drain off resources.

II. 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

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.

III. PROPOSED WORK

Various detection techniques have been proposed in MANET to eliminate the routing attacks.The main motto of this paper is to eliminate the routing attacks in Ondemand Dynamic Source routing protocol. As a result an Adaptive EADR approach is proposed to perform the detection and avoidance of attacks in the network layer.The Dempster Shafer theory is used for calculating risk assessment value.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

3.1 DYNAMIC SOURCE ROUTING PROTOCOL

There have been many routing protocols proposed to suit the different needs of MANETs. One of the most popular of them is Dynamic Source Routing protocol.There are two types of Routing protocols in MANET namely Proactive and Reactive. Of this DSR is a Reactive routing protocol which possess two phases namely Route Construction and Route Maintenance phases.During Route construction phase when node S wants to send a packet to node D, but does not know a route to D,node S initiates a route discovery. Source node S floods Route Request(RREQ). Each RREQ, has sender's address,destination's address, and a unique Request ID determined by the sender. Each node appends own identifier when forwarding RREQ.The destination node upon receiving a RREQ responds by sending a Route Reply packet back to source which carries the route transverse by Route Request packet received.

In the Route Maintenance phase it maintains a Route cache at intermediate nodes. An exponential back off algorithm is used to avoid frequent RouteRequest when the destination is in another disjoint set.The performance of DSR is compared to other routing protocols in MANET is shown in figure 2.

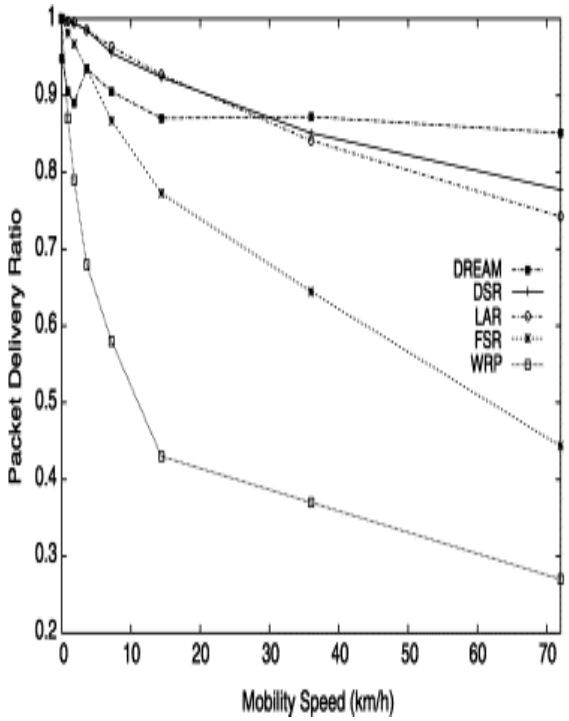

Fig 2 DSR Performance

3.2 ROUTE DISCOVERY USING DSR

The route discovery process takes place in this phase.The destination sends the request(RREQ) packet to source. The source node on receiving it floods RREP packet through the path traversed.Then the shortest path is discovered using DSR. Normally once the shortest route is established using DSR, the packets are then transmitted in the established shortest path.The attacker node is identified using Extended Dempster shafer theory.The risk assessment value is calculated using this theory.If an attacker node is present in that shortest path the attacker node duplicates the packets instead of intentional dropping of packets.These duplicated packets are sent to the destination node.Based on some criterias like Packet ID,secured secret key sharing the attacker node is detected on the destination side.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

3.3 AVOIDANCE AND ISOLATION OF ROUTING SALVAGE ATTACK

Initially bandwidth is assigned to each node.The bandwidth of every node is broadcasted to every other node in the network. Source node starts sending the data packet to next node in the route if the bandwidth of the next node is sent as a key to source node.Bandwidth value is also stored in route cache.If the value of bandwidth is true then the transmission takes place

IV. IMPLEMENTATION

The shortest route is ensconced by using Dynamic Source Routing protocol.The attacker node is detected in that shortest path. The Risk assessment value is calculated by using Extended Dempster Shafer theory.It is stated in **Eq 1**

$$E=(m_1+m_2,(IF_1+IF_2)/2)$$

- m-basic probability assignment function(**$m(\varphi)=0$**)
- IF-Importance factor

The detection of attacker node is shown in figure3.

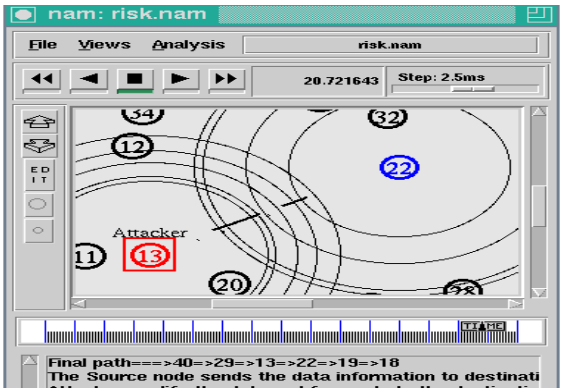

Fig 3 Detection of Routing salvage attack

4.1 SIMULATION METRICS

The essential metrics for a simulation environment is given in Table 1

Table 1
Simulation metrics

Packet size	256 bytes
Bandwidth	2 Mb/sec
Size of Square Area	800 X 800 m2
Average Forwarding Delay	1 ms
Transmission Range	50 - 300m

V. CONCLUSION

The attacks are the major threats to MANET.These types of attacks occur due to lack of fixed infrastructure.Currently several solutions are available for attacks that exists in MANET.In this paper we are able to provide a solution to routing salvage attack that occurs in the network layer.In this research effort we identified an efficient method to detect this attack and future works has been carried on providing solution.This approach increases the throughput, packet delivery ratio and reliability.

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 AdHoc 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 AdHoc 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 AdHoc 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.