EPTR: Energy Proficient Timestamp based Routing Approach, Survey and Analysis

Gayatri Bendale
Department of Computer Science & Engg.
Sri Aurobindo Institute of Technology
Indore,India
E-mail:bendalegayatri1@gmail.com

Prof. Sameeksha Shrivastava
Department of Computer Science & Engg.
Sri Aurobindo Institute of Technology
Indore,India
E-mail: sameeksha.shrivastava@sait.ac.in

***Abstract*—**Security has developed into a main anxiety in order to give protected communication among mobile nodes in a hostile environment. In current year with the extensive use of mobile device, Mobile Ad hoc networks (MANETs) technology has been attracted consideration day by day. Particularly, MANET suit for military operations and the developing disasters release that require to overcome environment and special reason in urgent. The reality that mobile ad-hoc networks lack fixed communications and use wireless link for communication makes them very disposed to an adversary's malevolent attacks. Black hole attack is one of the relentless security threats in ad-hoc networks which can be simply in employment by develop susceptibility of on-demand routing protocols such as AOMDV. In this paper, we are proposing an EPTR i.e. Energy Proficient Timestamp based Routing Method for detection and prevention of packet drop attack to defend network from malicious activity, compulsory by together single and manifold nodes. Result of a reproduction study proves the exacting resolution maximizes network appearance by minimizing production of control (routing) packets. The competence of our mechanism is demonstrated by reproduction conducted using network simulator NS-2.

***Keywords*-*MANET, AODV, Multipath, Packet Drop Attack, NS – 2, Routing, Security*.**

*****

I. INTRODUCTION

The ability to establish communication without an infrastructure and the capacity to communicate beyond the node's wireless transmission range embarks. With the fast growth and deployment of mobile devices, Mobile Ad Hoc Networks (MANETs) develop into a significant element of modern dispersed systems. As of the infrastructure-less property, MANETs preserve be simply deployed. They are very attractive to request such as military process and first response to disasters. These request, though, have very strict necessities on security of network topology and data traffic. Mechanisms should be properly designed for these applications previous to the compensation of MANETs can be fully oppressed [1].

In wireless ad hoc networks, nodes communicate with each other using multi hop wireless links. Data to out of range nodes can be routed through intermediate nodes. That is nodes in wireless ad hoc networks preserve act because together hosts and routers. There are numerous application areas in which wireless ad hoc networks can be used ranging from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during lectures [2]. The network topology might change with time because the nodes progress or adjust their broadcast and reception parameters. Thus, a MANET has some salient characteristics [3]

- Dynamic topology
- Resource constraints
- No infrastructure
- Limited physical security

The mobile hosts forming a MANET are usually mobile devices with limited physical fortification and income. Security modules, such as tokens and smart cards, preserve are used to defend after that to physical attacks. Cryptographic tools are widely used to provide powerful security services, such because confidentiality, authentication, reliability, and non-repudiation. Unfortunately, cryptography cannot guarantee convenience; for instance, it cannot put off radio jamming. For now, strong cryptography frequently demands a heavy computation overhead and need the assisting complex key allotment and trust management services, which typically are restricted by the capability of physical devices (e.g. CPU or battery)

1. Security attributes

Security is the mixture of procedure, measures, and systems used to guarantee discretion, verification, integrity, accessibility, admittance control, and non-repudiation [4] [5].

1.1 Confidentiality:

The goal of confidentiality is to remain the information sent incomprehensible to not permitted users or nodes. MANET uses an open medium, so typically all nodes within the direct broadcast range can find the data. One method to keep information private is to encrypt the data, and a different method is to use directional antennas.

1.2 Authentication:

The goal of authentication is to be capable to recognize a node or a user, and to be capable to put off consideration. In wired networks and infrastructure-based wireless networks, it is probable to implement a central ability at a point such since a router, base station, or admittance point. But there is no central ability in MANET, and it is much further difficult to authenticate an entity. Authentication can be achieved by using message authentication code (MAC).

1.3 Integrity:

The goal of consistency is to be capable to keep the message sent from being illegally distorted or destroyed in the broadcast. When the data is sent during the wireless medium, the data can be customized or remove by malevolent attackers. The malevolent attackers can furthermore resend it, which is called a replay attack. The integrity can be achieved by hash functions.

1.4 Non-repudiation:

The goal of non-repudiation is connected to a fact that if an entity sends a message, the entity cannot be against that the message be sent by it. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its classified key. All further nodes conserve authenticate the signed message by using A's public key, and A cannot deny that its signature is attached to the message

1.5 Availability:

The goal of availability is to keep the network service or income obtainable to legitimate users. It ensures the survivability of the network even with malicious event.

1.6 Access Control:

The goal of admittance control is to avert not permitted use of network services and system possessions. Obviously, admittance control is tied to authentication feature. In general, admittance control is the most commonly consideration of service in together network infrastructure and human being computer systems.

II.PACKET DROP ATTACK

In MANET, a packet dropping attack is a kind of denial of service in which a node in the network purpose drops the packets instead of forwarding them, which is exposed in the figure 1. The packet dropping attack [6], [7], [8] is very hard to identify and put off since it occurs when the node develop into cooperation due to a number of dissimilar causes. The packet dropping attack in MANETs can be confidential into some group in conditions of the strategy adopted by the malevolent node to launch the attack

- The malevolent node can on purpose drop all the forwarded packets going during it (black hole).
- It can selectively drop the packets originate from or designed to confident nodes that it dislikes.
- A special case of black hole attack dubbed gray-hole attack is introduced. In this attack, the malicious node retains a portion of packets, while the rest is normally relayed.

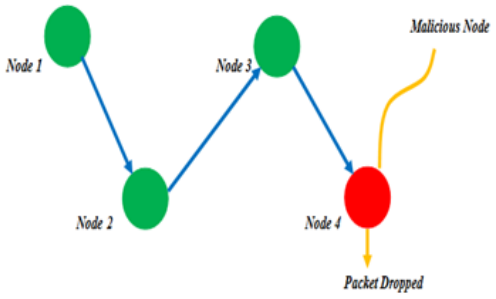

Figure 1: Packet Drop Attack

The compromised node will broadcast the message [8], [9] that it has the shortest pathway towards a purpose to initiate packet dropping attack. Therefore, all packet broadcast will be directed during the cooperation node, and the node is capable to drop the packets. If the malicious node attempts to drop all the packets, the attack can be known during common networking tools. Furthermore, when additional routers notice that the cooperation router is dropping all packets, they will classically begin to eliminate that router from their forwarding table. Then, there is no packet broadcast during the cooperation node.

III. LITERATURE SURVEY

Numerous Researchers have worked on manifold discovery and deterrence of wormhole attacks in wireless sensor network, based on the discovery mechanism, the accessible techniques of identify and put off wormhole attacks can be exemplify in this section.

Patcha [10] used a conservatory move toward to the watchdog move toward. In this move toward, the nodes in the network are confidential into trusted and normal nodes. The nodes which are worried in preliminary network formation are called because trusted nodes. The nodes which are mixture later in to the network are called as ordinary nodes. The ordinary node can be promoted as trusted node if the node demonstrates its honesty. A different supposition in this move toward is that all the trusted nodes comprise to not organism a malevolent or selfish node. The regulator nodes are selected from the set of trusted nodes for a known period of time based on the node energy, obtainable node storage ability and node computing power. The watchdog node has the additional responsibility to monitor additional nodes in the network for a fixed period of time to know the malicious behavior.

Deng et al. [11] presented a solution for solving problem of Black Hole Attack. In this technique, along with the RREP message, information regarding the neighbor of replying node is also asked and when RREP message reaches source, source instead of sending message immediately sends another message to neighbor of replying node asking whether the intermediate node which is replying for RREQ message really has path to destination or not. But it had limitation that it increased the message overhead so it can be used to verify identity of node which is under doubt of being malicious and it also assumed that Black hole nodes cannot work in group.

Raj and Swadas [12] proposed a method DPRAODV to detect black hole node based on RREP sequence number and threshold value. If the value of RREP sequence number comes out to be greater than the threshold value then the node sending this RREP will be considered as malicious. Further this malicious node is isolated from network by sending a control message ALARM to all other nodes and a list of blacklisted nodes is created. The reproduction consequences demonstrate that there was an increase in packet delivery ratio but also an increase in routing overhead and delay in message delivery.

Mistry et al. [13] did a modification in working of source node by the addition of new function for storing RREP messages for some specified time, a table which stores these RREP messages, a timer and Malicious node id for detecting black hole node and to keep record of all malicious nodes present in network. This technique discards the RREP message stored in table which has highest value of destination sequence number and node sending this RREP will be measured as malevolent and its identity will be stored as malicious id. This method leads to an increase in memory and time overhead but increase in packet delivery ratio compensated for that overhead.

Guori Li [14] with his colleagues uses sequential mesh test based scheme. The Cluster head node detects the nasty node based on the sequential mesh test method behind receiving the report from the nodes. In the scheme it extracts small samples from the networking nodes instead of doing test on whole

network in advance. In the sequential mesh test method, the test decides whether to continue the test or to hold after final conclusion.

Xin with his colleagues [15] uses light weight defense schemes for the detection of Gray Hole attack. He uses the neighbor node as monitoring nodes and resends the dropped packets again to the nodes associated with that node..

IV. PROPOSED SYSTEM

1. Problem Formulation

A problem domain is basically looking at only the topics of an persons interest, and exclusive of everything else. For the mainly improve obtainable work by finding base problem.

- Link failure is a main problem in AOMDV which is dependable for the poverty of the network and packet drop. There are number of nodes in the network where source is host node from where data is send and destination node is the final node. Throughout link failure, the resource node is informed regarding the failure in the network so that moreover it might slow down the packet broadcast rate or discover an alternate route which might not essentially be an best route. Another problem is that congestion control. Congestion control is a key difficulty in mobile ad-hoc networks. Overcrowding has a severe impact on the throughput, routing and presentation and additional routing functionalities.
- In MANET, Multiple route are available, if communication being happened through AMODV for communication, amongst node where no one link is established until RREQ and RREP process is done in predefined timestamp. So there is more chances most of the node consume high energy constraint when there is malicious link is available. For this we are proposing a new scheme for defending packet drop attack an Energy proficient Multipath Routing Method where node timestamp is calculated to preserved system performance and reduce end to end delay and particularly node energy

1.2. Proposed Solution

In case of MANET the number of nodes is can growth freely in the area since there is no central organizer in the MANET. It is self-configuring system. So whilst the data is send from resource to purpose packet drop is high considerably and Link failure problem occur due to free or simply arrangements of the nodes.

Wireless networks are very simple to deploy since there is no require ascertaining any physical path. This feature of wireless network results into birth of various attacks. In the Packet drop attack, the attacker targets some nodes in the wireless network and then drop the packets sent towards the intended nodes. Attackers try to drop/delay the packets in the routine manner

To overcome and reduce the above problem of network various techniques of multipath routing method had been proposed in the prior times. Between all the proposed techniques multipath routing is the majority resourceful and progressive technique for improvement of network performance in effective mobile ad-hoc networks.

In this work, we will improve the Detection rate of the attack at the same time when packets are forwarded from single source to multiple destination followed by multipath routing scenario in MANETs. The improvement will be based on the definite values of the Timestamp. In this work, development of the proposed method resolve is done to amplify its competence in terms of energy, end to end delay, throughput and PDR.

V. CONCLUSION

Security which is a critical factor is a concern in these kinds of networks due to lack of centralized control. In recent years the widespread availability of wireless communications, mobile computing and handheld devices has led to the growth and significance of wireless mobile ad hoc networks. Though there have been many works in the recent years on secure routing protocols. This survey paper initiate key defense threats in MANET and moreover discover Black-hole attack discovery and deterrence technique, and how these solutions are capable to safe the network therefore the finally, by approximation the pros and cons of obtainable technique the open investigate challenges in mobile ad-hoc network are studied Oct 2009

REFERENCES

[1]. Wang, Weichao, Bharat Bhargava, and Mark Linderman, "Defending against collaborative packet drop attacks on MANETs," 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, Volume 2, 2009.
[2]. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 2004
[3]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions, IEEE Wireless Communications, pp. 38-47, 2004.
[4]. PRADIP M. JAWANDHIYA, MANGESH M. GHONGE and DR. M.S.ALI, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), PP. 4063-4071, 2010.
[5]. A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[6]. S. Djahel, F.N. Abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals and Challenges, IEEE Communications Surveys & Tutorials, Vol.13, No.4, Fourth Quarter 2011.
[7]. E. Hernandez, M.D. Serrat, Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog, IEEE Communications Letters, Vol.16, No.5, May 2012
[8]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conference II WAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.
[9]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
[10]. A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.
[11]. H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazines, vol. 40, no. 10, October 2002.
[12]. P.N. Raj, P.B. Swadas, "DPRAODV: A Dynamic Learning System against Black Hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.
[13]. N. Mistry, D.C. Jinwala, M. Zaveri, "Improving AODV Protocol against Black hole Attacks", in Proc. of the International Multi Conference of Engineer and Computer Science, Vol. 2, 2010.
[14]. Gouri Li, Xiangdong Liu and Wang″ A Sequential Mesh Based Test based Selective Forwarding attack, detection schemes in wireless Sensor Nrtworks".
[15]. Wang Xin-Sheng, Zhan Yong-Zhao, Xiang Shu-ming and Wang Liangmin, ″Lightweight defense scheme against selective forwarding attack in Wireless Sensor Networks" pg 226-232.