Security Approach Regarding Routing Protocol for Network Layer in MANET

S.V.Shirbhate Dr.S.S.Sherekar Dr.V.M.Thakare

Abstract **:- Mobile Ad hoc Network is one of the most promising technologies that have applications ranging from emergency disaster up to sharing information during conference. Although MANET have appealing features such as dynamically establish their own network without relying on any central administration, due to frequent topology changes caused by nodes mobility, as well as unreliability and bandwidth limitation of wireless channels, the security of such network is a big concern, especially for applications where confidentiality has prime importance. Therefore in order to operate in MANET as a secure way, any kind of intrusions should be detected before attacker can harm the network.**
As a security point of view, it is needed to revise and analyze the recent development of security mechanism such as primitive, incentive and detection/reaction approaches for securing the mobile network to acquire the direction of future research. This paper focuses on various routing protocol attacks and overviews of security schemes against the intrusions.

Keywords **: MANET, Intrusion detection, preventive, Incentive.**

I. INTRODUCTION

Mobile ad hoc network is a temporary infrastructure less network, formed by set of wireless mobile hosts that are dynamically establish their own network without relying on any central administration. Due to this features it can be applied in various areas such as emergency disaster relief in damaged area after a storm or an earthquake; a set of digital sensors positioned to take measurements in a region unreachable by humans; military tanks and planes in a battlefield; and researchers sharing the information during a conference [1]. Although it can be applied in various areas, because of vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and lack of a centralized monitoring or management point, security in mobile ad hoc network is difficult to achieve. Previous studies on mobile ad hoc network are designed at proposing protocol for some fundamental problems such as routing and tried to deal with challenges imposed by new environment. However, these protocols fully trust all nodes and do not consider security aspect. As a result they are vulnerable to attack and misbehavior.

In a MANET, each node participates in an ad hoc routing protocol that allows it to discover multi-hop paths through network from itself to destination i.e. each node can be act as router that discover and maintain routes to the other nodes in the network. The main aim of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. If routing can be misdirected, the entire network can be paralyzed [2]. In this way routing security plays a vital role in the security of whole network.

II. ROUTING PROTOCOL SPECIFIC ATTACK

In a MANET the routing protocols are classified according to information is exchanged into three types; proactive, reactive and hybrid. Proactive protocol is also known as table driven protocol because these protocols require each node to maintain one or more tables to store routing information. Each type of protocols performs differently under different network scenarios. Proactive protocols maintain routing information for all mobile nodes and keep updating information periodically in order to maintain a consistent network view. In such way route discovery overheads are large in proactive routing protocol e.g. DSDV whereas reactive protocols instead of maintain routing information, they discover the path to the destination on demand. This is also called as on demand protocol. In this way it saves memory, battery power and bandwidth for e.g. AODV. Hybrid protocols combine the advantage of both proactive and reactive protocols e.g. TORA. Although the intention of routing protocols is to establish a correct and efficient route between a pair of nodes, they are vulnerable to routing attack because of the assumption that all the nodes cooperate to find the best path. Consequently, a malicious node can exploit the vulnerabilities of cooperative routing algorithms and lack of centralized control can caused to initiate routing attacks [3]. The following section elaborate on the different intrusive activities can cause various attacks in MANET by regarding on demand routing protocol (AODV).

2.1 Sleep Deprivation Attack

It is a distributed denial of service attack in which an attacker can interacts with the node in a manner that appears to be legitimate; however the purpose of interaction is to keep the victim node out of its power conserving sleep mode. In [4] the authors consider an intruder can cause sleep deprivation attack by exploiting the vulnerabilities of route discovery process of protocol through malicious route request (RREQ) flooding. In such attack an intruder broadcast a RREQ with destination IP address that is within the network address range but where the corresponding node does not exist and force all the nodes to forward this RREQ. After broadcasting a RREQ an intruder does not wait for ring traversal time, but it continue resending RREQ for same destination with higher TTL values. In this way it is a DDoS attack for conserving the power.

2.2 Black Hole Attack

In this attack, when a node requires route towards the destination, intruders can exploit the vulnerability in route discovery procedures of on demand routing protocols. When the node sends RREQ, an intruder advertises itself as having fresh route. In this way once the intruder is chosen as an intermediate node, it drops the packet instead of forwarding or processing them causing black hole attack in the network [5].

2.3 Grey Hole Attack

It is a special type of black hole attack, in which an intruder first captures the routes and becomes part of the routes in the network then drop packets selectively. The packet dropping attack is different from the black hole and gray hole attack. In packet dropping attack the attacker simply fail to forward packets for some reason whereas in black hole or gray hole attack, the attacker first captures routes and then either drops all or some packets[3].

2.4 Rushing Attack

In on demand routing protocol, with the intention of limit the control packet forward, a node requires to forward only the first RREQ that arrives for each route discovery. An attacker can exploits this property by spreading RREQ packets quickly throughout the network to suppress any afterward legitimate RREQ packets. For example in AODV routing protocol, an intruder can forge and forward a rushed RREQ by assigning a higher source sequence to it. Also an intruder transmits the packet earlier than specified in AODV protocol. Due to this any later legitimate RREQ to be suppressed and increases the probability that routes that intruder will be discovered instead of valid routes.

2.5 Sybil Attack

In MANET for identification purpose each node requires a unique address to participate in routing. Still in a MANET there is no central authority to verify these identities. An attacker can exploit this property and send control packets such as RREP or RREQ using different identities. This is known as Sybil attack which impersonates to create confusion in routing process or base for other severe attack by using random identities or identity of another node.

In such a way Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process [6].

III. MECHANISM FOR SECURING ROUTING PROTOCOL

From above discussion, routing attacks are particularly serious in MANET. As a security point of view in MANET, many investigations have been done. Basically there are three defense lines to protect the MANET against the network layer attacks as shown in fig 1. The first defense line is prevention try to prevent the malicious node from participating in routing activities such as packet forwarding function. When malicious node exceeds this fence second defense line incentive is launched. In incentive approach, search is to encourage the cooperation among the router nodes by means of an economic model. Finally both the line of defense fails the third line of defense i.e. detection and reaction is launched to disclose the identity of the malicious node and excludes it from the network.

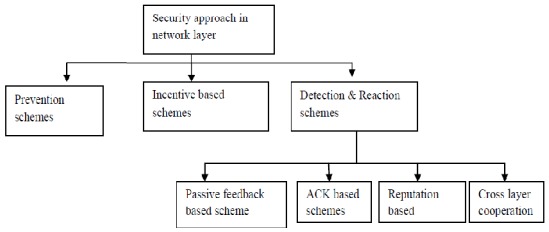

Fig. 1 : defense line scheme

3.1 *Prevention scheme*

In prevention based security approach, many researchers have been interested to develop mechanism to identify malicious node that attempt to involve them in the routing path and then take control over data/control packets. For example cryptographic and authentication technique is used to prevent the attack.

3.2 *Incentive based scheme*

There are some nodes which do not want to waste its resources for benefit of other nodes. Therefore it refuses to forward others packets however it still uses their services to communicate. Such a problem is solved by denying such a node from the services provided by the rest of the network. Therefore it will be obliged to cooperate. Otherwise it will be isolated from the network and never get its packets forwarded. Such a solution is referred to as incentive based scheme.

3.3 *Detection and Reaction Approach*

The detection and reaction scheme identify and prohibit the malicious node. It is further classified into passive feedback, Acknowledgement, reputation and cross layer cooperation based scheme.

Passive feedback schemes enclose all the solutions whose principle consists in overhearing the neighbor's transmission to check its legitimacy. In acknowledgement based schemes, a node might request an acknowledgement from its succeeding neighbors to conform the well reception of its packet. In reputation based scheme the judgment of the malicious or normal node according to an assessment of its trustworthiness level which is computed based on several observations of its behavior. In cross layer cooperation based schemes, two or more layers are cooperated to detect or enhance the detection accuracy [1]. The following section analyzed and discusses on various security approaches in network layer.

IV. ANALYSIS AND DISCUSSION

Although cryptography schemes are efficient to several properties such as confidentiality, data integrity and non repudiation, in MANET it cannot be adopted since these techniques cannot prevent malicious node from dropping packets [1].

In [7] the authors proposed a solution to survive with the black hole attack in which AODV reactive routing protocol is used. Authors suggest disabling the ability of an intermediate node to RREP and allowing only the final destination to do that. According to this scheme it avoids the black hole attack however in case of large network; it increases the route establishment delay. Furthermore since no authentication is used in RREP message, a smart attacker can forge a RREP message on behalf of the legitimate destination. To overcome this problem authors proposed another solution which requires that intermediate node adds its next hop information to RREP packets before sending it. On receiving the packet, the source node send a special packet to the next hop of intermediate node in order to verify that it has route to destination and also it is a neighbor of the intermediate node. The special packet contains a double check result which is filled by next hop node. When the source node receives this reply, it checks the result information and decides whether the route is safe or not. This solution avoids the black hole attack launched by single node but fail to detect the collusive attack carry out by intermediate and next hop node. Moreover this solution requires a communication overhead.

[8] Propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. Authors focus on detecting malicious links instead of malicious nodes. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the path. Each packet sender maintain the list of identifier of data packets that have been sent out but have not been acknowledge yet, a counter of forwarded data packets and a counter of missed packets. According to the value of acknowledgement ratio, only fraction of data packets will be acknowledge in order of reducing additional routing overhead.

[9] Propose artificial intelligence based learning technique to synthesize the most appropriate intrusion detection programs for the challenging network type. It detects known flooding, and route disruption attacks. In Grammatical Evolution, a problem is defined with the Backus-Naur Form (BNF) grammar and the fitness function. Mobility related features as well as packet related features are taken as input to the evolution system.

In [10] paper authors propose a trust-based security extension to the mobile ad hoc network dynamic source routing protocol (DSR), where the state probability of a node, according to its corresponding hidden Markov model (HMM), is being used for deciding the node's trustworthiness. In this method each node in the MANET monitors all of its neighbors and uses an HMM to decide and predict whether or not each neighboring node is selfish.

In [11] approach, by using the redundant routing information that is naturally present in an ad hoc network, prevents the diffusion of malicious RREP messages in the network. In this technique each wireless node embeds the inner circle framework, which is on outline to intercept incoming/ outgoing RREP messages and to run a deterministic voting service that checks the validity of received RREP messages. During the voting algorithm execution, each node of an inner-circle node verifies the validity of inner circle node RREP message according to check function. Node of inner circle agrees only if inner circle node is the destination of the sought route or nodes of inner circle node considers as a valid forwarding node to the destination and both inner circle node and RREP message's next hop are authenticated neighbors of node of an inner circle nodes.

In [12] paper authors present an integrated secure routing system based on Intrusion Detection Systems (IDS) and Statistically Unique and Cryptographically Verifiable (SUCV) identifiers. The proposed IDS has been used for the support of secure Ad Hoc On Demand Distance Vector (AODV) routing, named IDS-based Secure AODV (IS-AODV), in wireless ad hoc and vehicular network scenarios. This Intrusion detection system is based on the detection of behavior anomalies on behalf of neighbor hosts, with passive reactions, aiming to create a *cluster* whose route paths will include only safe nodes.

A summary of the characteristics of the surveyed schemes is presented in above Table I. This table emphasizes the most prominent features of security scheme in terms of scalability, overhead and the reaction mechanism adopted to exclude the detected attackers. Moreover this table also focuses on weak point of each scheme. The feature of each scheme are highlighted based on the following metrics

- Security mechanism to which the scheme belongs.
- The overhead generated by the scheme in terms of new packet sent and extra computation required carrying out the scheme.
- Which method is used to detect the intrusion ?
- The architecture of the scheme
- Which technique or algorithm is used to detect the intrusion?
- Is the scheme providing any reaction technique to punishment the detected attacker?
- The impact of routing protocol performance such as end-to-end delay and packet delivery ratio
- Is the scheme scalable to large network?

V. CONCLUSION

Security in mobile ad hoc network is complicated to achieve, especially from network layer attacks since the flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices introduces new security risks. This paper focuses on significant network layer attacks and reviewed security mechanism that have been proposed in literature. The literature review shows that intruders find new ways to attack and cause damage to the system and networks. So there is a need to allow a protection mechanism to learn from experience and knowledge of attacks to infer and detect a new attack is an imperative and probably fruitful area of future research. The improvement and exploitation of network security strategies are important in network with dynamic environment is a further potential area of research. The attacker may try to attack an existing protection scheme therefore there is a need of a robust protection mechanism to protect and not introduce new vulnerabilities into the network.

Author	Security Mechanism	method	Architecture	ID techniqu /algorithm	Attack/Attacks	Routing protocol	Source of data	Computational overhead	Communication overhead	Scalable	Weakness	Response modu
Hongmei Deng and et.al. [7]	Acknowledgement based approach	Disable the ability to reply the a message of an intermediate node	Distributed	Reply RREQ messages to check whether the route from intermediate node to the destination node exists or not.	Black hole	AODV	Routing and packet related features	Low	High	No	It is unable to detect a collusive attack conducted by intermediate and next hop nodes	Send out alarm message to the and isolate the no the network.
Sevil Sen and et.al[9]	Detection /Reaction approach	artificial intelligence based learning technique	Distributed	The grammatical evolution technique	Dropping Attack, Flooding Attack and route disruption attacks.	AODV	mobility-related features and packet related features	High	No	Yes	Detect the intrusions but other factors such as resources used by programs are not consider	Not consider
Marie E. G. Moe and et al.[10]	Reputation based approach	Trust-based security	Distributed	hidden Markov model	selective packet dropping	DSR	Observed and overhearing transmissions of nodes in the environment.	High	Low	No	Overhead induced in sharing reputation information amongst the nodes	Enforcing coo among nodes removing the i for selfish node be
Kejun Liu and et.al. [8]	acknowledgement based approach	Two hop acknowledgment packets	Not mentioned	Add-on technique for routing protocol DSR	Detect the misbehaving link instead of node	DSR	List of data packets ID's.	High	High	Yes	The 2ACK scheme can only work in managed MANETs not in open MANET	Broadcast the message misbehaving link it to the blacklist way avoid misbehaving link part of its route.
Claudio Basile and et.al. [11]	Other schemes	Threshold cryptography(fault-tolerant cluster algorithm)	Stand alone	Integration of Statistical and security technique	Packet dropping attack (Blackhole)	AODV	Routing and packet features	High	High	Yes	Determining the threshold is a complex task.	Diffusing a malicious message for a des and valid rou established
Luciano Bononi and et.al[12]	Passive feedback schemes	Intrusion Detection Systems (IDS) and Statistically Unique and Cryptographically Verifiable (SUCV)identifiers.	Stand alone	Anomaly intrusion detection technique (IS-AODV)	Detect misbehaving host. Not the specific attack.	AODV	Captures all the node traffic	Low	Low	No	Assume that source and destination node is normal. however if source or destination node is malicious then this method will not work properly.	Isolating mi hosts, and create whose route p include only safe

REFERENCES

[1]. Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang, "Security Approach Regarding Routing Protocol for Network Layer in MANET", IEEE Communications Surveys & Tutorials, Vol. 13, No. 4, Fourth Quarter, PP.648-672, 2011.

[2]. S.V.Shirbhate, Dr V.M.Thakare ,Dr S.S.Sherekar, "Security In Routing Protocol for Mobile Ad Hoc Network", National Conference On Innovative Paradigms in Engineering & Technology (NCIPET),PP. 437-443, February 2013.

[3]. Adnan Nadeem, and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter, PP.2027-2045, 2013.

[4]. Adnan Nadeem and Michael Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs", ACM 978-1-60558-569-7/09/06, IWCMC'09, PP.926-930, 2009.

[5]. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Tansactions On Vehicular Technology, Vol. 58, No. 5,PP.2471-2481, 2009.

[6]. Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE Systems Journal , Vol. 7, No. 2,PP.236-248, 2013.

[7]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine 0163-6804/02, PP.70-75, 2002.

[8]. Kejun Liu, Jing Deng, , Pramod K. Varshney, , and Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transaction on mobile computing, Vol. 6, No. 5,PP.536-560, MAY 2007.

[9]. Sevil Sen, John A. Clark, "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks", ACM 978-1-60558-460-7/09/03, PP. 95-102,2009.

[10]. Marie E. G. Moe, Bjarne E. Helvik, Svein J. Knapskog, "TSR: Trust-based Secure MANET Routing using HMMs", ACM 978-1-60558-237-5/08/10, PP.83-90, 2008.

[11]. Claudio Basile, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Inner-Circle Consistency for Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 6, No.1, PP.39-55, 2007.

[12]. Luciano Bononi and Carlo Tacconi, "Intrusion detection for secure clustering and routing in Mobile Multi-hopWireless Networks", Int. J. Inf. Security,in Springer, DOI 10.1007/s10207-007-0035-9, 6, PP.379–392 ,2007.