Security in Routing Protocol for Mobile Ad Hoc Network

S.V.Shirbhate
Research scholar
Amravati.

V.M.Thakare, Ph.D
S.G.B.A.U.
Amravati

.U S.S.Sherekar, Ph.D
S.G.B. A.U
Amravati

ABSTRACT

Today's mobilizing world, corporation and government agencies are progressively used embedded and wireless technologies. Since the advent of wireless communication, the need for mobile ad hoc networks has been growing exponentially. MANET is a developing research area with applied applications. Due to fundamental characteristics of MANET, it is useful and more popular in mobilizing world. But these features such as open medium, dynamic topology, distributed cooperation and constrained capability are particularly vulnerable to MANET. The security is one of the important challenges in MANET. MANET's topology poses many new challenges such as routing problem which can be solved by routing protocols. Routing plays an important role in security of the entire network. Routing is the central part of wireless ad hoc network. This paper focuses on the routing protocols and some of the vulnerabilities, specifically discussing attacks against routing protocol and analyzes the role of routing protocols in security.

Keywords

Wireless Technology, Routing Protocol, MANET, Security.

1. INTRODUCTION

Now a day there is a tremendous growth in mobile devices. As the increment in mobile devices, the basic need to share information is also increases. As initiation of wireless communication, the need for mobile ad hoc network has been growing exponentially. MANET is an infrastructure less network in which each node participates in an ad hoc routing protocol that allows it to discover multi hop paths through network [1]. In ad-hoc network routing protocols are central. Routing functionality i.e. all the network activities including discovering topology and delivering messages must be executed by the mobile nodes in ad-hoc network. Comparatively Ad hoc network is different from wired network. It has limited bandwidth, limited battery power and dynamic topology. In traditional wire line network, there are several approaches in conventional routing algorithm some of them are also used in ad-hoc network such as link state, distance vector, source routing and flooding. Basically there are three types of routing protocols used in MANETs namely: proactive, reactive and hybrid routing protocols [1]. Although a majority of these protocols assume a reliable collaboration among participating devices, identification shortcomings in the protocols, the lack of conventional and authentication mechanisms causes security problem [2]. A critical system having secure communication required not only intrusion prevention but also intrusion detection play a vital role to satisfy the security requirement [3]. The characteristics of the ad-hoc network are vulnerable to various kinds of attacks. Hence there is need to detect the malicious node and response mechanism in order to protect the individual nodes in mobile ad hoc network [2]. In such a way deploying Intrusion Detection Systems (IDSs) for Mobile Ad hoc Networks are indispensable [3].

The remainder of the paper organized as follows, section II elaborates the classification of routing protocols, section III describes the attacks in routing protocol, section IV describes security in routing protocol and section V contains tabular form of security in routing protocol and discussion. Finally at the section VI conclude by discussing the outcome of study.

2. CLASSIFICATION OF ROUTING PRTOCOLS

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 [4]. In this way routing security plays a vital role in the security of whole network.

In a MANET the routing protocols are classified according to information is exchanged into three types; proactive, reactive and hybrid as shown in fig. 1. 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 [5] 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 [1] for e.g. AODV. Hybrid protocols combine the advantage of both proactive and reactive protocols e.g. TORA. Following are routing protocols used in MANET.

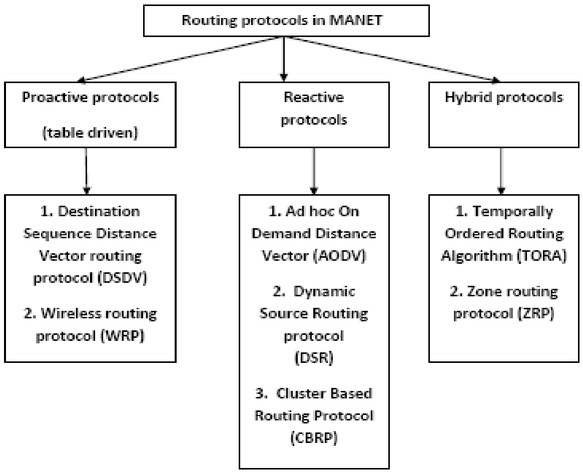
Routing protocols in MANET
Proactive protocols (table driven)
Reactive protocols
Hybrid protocols
1. Destination Sequence Distance Vector routing protocol (DSDV)
2. Wireless routing protocol (WRP)
1. Ad hoc On Demand Distance Vector (AODV)
2. Dynamic Source Routing protocol (DSR)
3. Cluster Based Routing Protocol (CBRP)
1. Temporally Ordered Routing Algorithm (TORA)
2. Zone routing protocol (ZRP)

Fig. 1. Classification of routing protocol in MANET

2.1 Destination Sequence Distance Vector (DSDV)

It is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. This algorithm solves the routing loop problem which is present in Bellman-Ford algorithm. For this it uses a sequence number [5]. In this routing protocol each mobile node in the system maintain routing table in which all possible destination and number of hops to them in network are recorded [1]. Each entry in the routing table contains a sequence number; the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently [1][5].

2.2 Ad hoc On demand Distance Vector (AODV)

It establishes a route to a destination only on demand. When there is no need of a connection, the network remains silent. It is a distance-vector routing protocol. AODV avoids the count to- infinity problem by making use of sequence numbers [5]. When a connection is needed, the network node that needs the connection broadcasts a request for finding a route to the destination. Other nodes forward the message, and record the id of the node that they heard it from, creating temporary routes back to the needy node. When a node receives such a message and already has a route to the destination, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops to the destination. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

2.3 Temporally Ordered Routing Algorithm (TORA)

It is hybrid protocol which combines the advantages of both proactive and reactive protocols. TORA does not use a shortest path solution. It builds and maintains a Directed Acyclic Graph rooted at a destination. No three nodes may have the same height. TORA makes use of height in order to prevent loops in routing. Information may flow from nodes with higher heights to nodes with lower heights, but not vice versa [1].

2.4 Dynamic Source Routing Protocol (DSR)

DSR is a reactive or on demand protocol. In which the sender of data packet find the source route i.e. full path from sender to receiver and includes in the packet header. The intermediate nodes used this information to determine whether they accept a packet and where to forward it. This protocol operates on route discovery and route maintenance mechanism [5] [6]. DSR is different from AODV in the sense that each mobile node keeps the track of the routes of which it is aware in a route cache. Upon receiving a search request for path it consults with its route cache to see it contains required information. This protocol uses more memory but reducing the route discovery delay in the system [4].

2.5 Zone Routing Protocol (ZRP)

Zone routing protocol is hybrid protocol which act as proactive as well as reactive according to the need of application at a particular instances of time depending on the prevailing scenario. In ZRP local neighborhood are called zones where each node may be within multiple overlapping zones and having different sizes. The size of the zone is measured by radius of length α. Where α is number of hops to the perimeter of the zone. ZRP consist of three parts IARP (Intrazone routing protocol), IERP (Interzone routing protocol) and BRP (Border cast Resolution protocol) with IERP. IARP is a proactive part whereas IERP is a reactive part and BRP with IERP is used to reduce the query traffic. Here [7] author analyzing zone routing protocol in MANET against authentic parameter such as throughput, average End to End delay, average jitter effect, packet loss percentage by varying various attributes such as zone radius and node density. Result show that in high density node ZRP having higher zone radius gives better throughput, smaller zone radius increases end to end delay, smaller zone radius increases average jitter and smaller zone radius increases packet loss in high density node.

2.6 Clustered Based Routing Protocol (CBRP)

It is as on demand routing protocol which divides the clusters into nodes and decreases control overhead during route discovery [8]. Cluster based routing protocol have advantages over other protocols such as it uses multiple channels effectively and improves system capacity, reduces the exchange overhead of control messages and strengthens node management, very easy to implement the local synchronization of network, provides quality of service routing for multimedia services efficiently and support the wireless networks with large number of nodes [8]. There are also various kinds of protocol such as Location Aided Routing (LAR) in which GPS is used for location information it reduces the search space for desired route, Improved Location Aided Cluster based routing protocol (ILCRP) is stable clustering protocol. This protocol makes the use of clusters as well as location information.

3. ATTACKS IN ROUTING PROTOCOL

For effective operation in MANET it is needed to maintain the appropriate routing information in a distributed manner. Unfortunately there is no such security is considered in routing protocol. Due to this reason routing protocols are easily targeted by the attackers. Attacks on MANET routing protocol are classified into two types according to the routing functionality.

3.1 Traffic Distortion

This is a passive attack which does not disrupt the operation of a routing protocol. It can snoop network traffic, manipulate or corrupt packet header or contents, block certain types of traffic or replay transmission for some malicious purposes [4] [6]. Examples of such type of attacks are packet dropping which may be random, constant, periodic and selective dropping. Another example is identity impersonation.

3.2 Route Logic Compromise

This is an active attack which improperly modifies data, gain authentication or acquire authorization by injecting false packet into the data stream or modifying packet transition through network to disrupt or damage route fabrics. It can be further divided into external attack and internal attack [4] [6]. External attacks are launched from the outside of the network whereas internal attacks are initiated by one or more compromised nodes belong to the network. Internal attacks are more critical since malicious nodes are already belonging to the network as authorized parties. Therefore such nodes are protected by the network security mechanism and underlying services. Internal attacks coming from compromised nodes have a severe impact on network performance and its connectivity. Therefore detecting internal attacks launching from these compromised nodes is indispensable [9]. Examples of active attacks in network layer are black hole, worm hole, DoS, impersonation, information disclosure ,energy consummation and specifically routing attacks such as routing table overflow, poisoning, packet replication, route cache poisoning, rushing attack [10].

4. SECURITY TECHNIQUES IMPLEMENTED IN ROUTING PROTOCOL

The functionality of router in any routing protocol is that establishing route path for future path packet delivery and forwarding data packets based on established routes. Ultimately all attacks on routing protocols achieve their goals by compromising at least one of the routing functionalities. Hence collecting and analyzing proper routing and traffic related measures can detects possible attacks to the routing protocol. Secure ad hoc routing protocol is one of the techniques to enhance the security in MANET. There are various prevention schemes to secure the ad hoc routing protocol i.e. authentication and encryption schemes. However these schemes cannot eliminate all intrusions occur in routing protocol hence there is need of intrusion detection and response system as second line of defense to secure routing protocol [5]. Basically intrusion detection technique classified into three types based on detection technique; misused or signature based, anomaly and specification based intrusion detection technique. In [11] analyzes some of the vulnerabilities, specifically discussing attacks against AODV that manipulate the routing messages. In which authors propose a solution based on specification-based intrusion detection to detect attacks on AODV. Momentarily, this approach involves the use of finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. The simulation results indicate that the proposed approach can effectively detect most of the serious AODV routing attacks effectively with low overhead. In [1], DSDV, AODV and TORA routing protocols are compare in terms of convergence time which is the time between fault detection and restoration of new, valid, path information. Here authors also specify in which situation these algorithms have their strengths and weaknesses for example AODV providing fast convergence with low node densities and high mobility whereas DSDV performing well with high node density and low mobility.

To protect against black hole attack in [4] propose a feasible solution for it in AODV protocol. For detecting attack it requires the intermediate node to send a RREP packet with next hop information. When source node receives RREP packet from an intermediate node, it sends Further Request to the next hop to verify that it has route to the intermediate node that sends back the RREP packet and it has route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route.

In [6], a new data mining approach based on cross feature analysis is used for detecting routing anomalies in MANET. AODV and DSR routing protocol are used. This approach is very useful when strong inter feature correlation can extracted automatically in normal system data.

In [8], protocol ILCRP with IDS is proposed. It uses distributed cluster based IDS with GPS enabled nodes. Due to energy constraint, cluster head selects node with second highest node value as monitoring node to captures live packet traffic on the network. All member nodes of cluster act as sensor to obtain audit data and forward to the monitoring node of cluster. Fusion model combines all audit data. Detection and analyzer module (DAM) is analyzing audit data, monitoring node detects any malicious activity in the path of nodes between source and destination by using rule such as; interval, transmission/retransmission, and delay rule. After detecting malicious node cluster head marks that node as the blacklisted node and add it to the blacklist. Then blacklist broadcasts to all member nodes of cluster.

5. ANALYSIS AND DISCUSSION

Following table1 gives the analysis of security in MANET by using various routing protocols. Here analysis will be done on the basis of routing protocols used for detecting various routing attacks, various methods and techniques for detecting routing attacks. This table also analyze various parameters used for detecting routing attacks and discuss the result on the parameter.

Author name	Year of publication	Routing protocol & network simulator	Attacks	method	Tech.	Parameters .	Result
Hongmei Deng et. Al	2002	AODV (NS2)	1.Black Hole	Reply RREQ messages to check whether the route from intermediate node to the destination node exists or not.	Securing AODV protocol	False positive rate and detection rate	Increased throughput i.e. increased detection rate and minimized false positive rate
S.Mangai et al	2011	ILCRP (NS2)	1.Black hole 2. worm hole and 3. node impersonation	Detecting intrusion by using location information with security against attack	Distributed cluster based IDS with GPS enabled nodes	Packet delivery ratio & control overhead	Comparative study shows that packet delivery ratio is higher in ILCRP with IDS than ILCRP. But control overhead increases in ILCRP with IDS.
Baolin Sun et al.	2005	secured AODV (SAODV) NS2	1.Attacks on AODV Routing protocol (Routing disruption attack)	A network monitor Employs a finite State Machine (FSM) for detecting incorrect RREQ and RREP messages	Specification based Intrusion detection technique to monitor AODV	Control overhead, delivery ratio, percentage of RREP forwarded	Effectively detects AODV routing attacks. Comparison between AODV and SAODV shows that, SAODV increases overhead, but average delivery ratio less than AODV due to overhead. When attackers exist, packet drop ratio is less in SAODV i.e. attackers are less effective against SAODV
Yi-an Huang et.al.	2003	DSR AODV (NS2)	1.Black hole and 2.selective packet dropping attack	Cross feature analysis method to find inter correlation	data mining approach	AMC (average Match Count) & AP (Average probability)	Effectively detects anomalies caused by typical routing intrusions
Bo sun	2003	DSR (GloMosim)	1.routing disruption attack	detection algorithm	Markov chain based anomaly detection algo	Mobility level	1.Low false $+^{VE}$ ratio 2. High detection ratio 3. Small MTFA (mean time to first alarm) When mobility is low

Table 1: analysis of security in MANET based on routing protocol

By using security provided in AODV method [4], black hole attack is avoided and also prevents the network from further malicious behavior. But this method increases the routing overhead due to the check process to every intermediate node that sends REPLY message. It means that this method is applied in situation where nodes are suspected. To find the suspected node Internal Attack Detection Model (IADM) is used.

In ILCRP with IDS [8], location information of the nodes makes the packet route, loop free which results in high packet delivery ratio. But control overhead increases due to monitoring all nodes as well as cluster head. ILCRP is not affected by worm holes due to its location based information and also node impersonation does not occur due to use of long and permanent identifier for each node. Since IDS is performed collectively, the energy consumption is further reduced.

Data mining approach based on cross feature analysis for anomaly detection in MANET routing [6] is very useful when strong feature correlation can be extracted automatically in the normal system data. In this model, duration of each intrusion session and the gap between two adjacent intrusion sessions are the same. The value of duration is specified as a script parameter but detection performance is not investigated for different set of period values.

In [3], an intrusion detection agent is attached to each node to monitor the activities to detect abnormal behavior. Here Markov Chain based anomaly detection algorithm is implemented. Because of random mobility in MANET, it is very difficult to establish a mathematical model to characterize routing disruption attack. Also, if the attacker only sends one or two falsified routing control packets, it is very difficult for the victim to tell whether these falsified routing control packets are caused by mobility induced errors or generated by attackers, based only on the local communication activities. All of these pose challenges to the detection of routing disruption attack.

The above security approaches in routing protocols have advantages and limitations. Routing protocols are the cornerstone of MANET. Improper and insecure routing mechanism will not only degrade the performance of network but also makes network vulnerable to many security attacks. One of the basic elements in routing mechanism is routing message which is used to establish and maintain the relationship between the networks. Hence to secure routing protocol, it is a need to explore a technique that may employ in protecting, detecting and responding to the attacks against the routing messages.

6. CONCLUSION

The MANET is a challenging research field with real-world applications. Although due to its features like dynamic topology, open medium, distributed corporation, constrained capability and flexibility MANET supports the various applications, but these features affects the security of the system. Routing security plays a vital role in the security of the entire network. In wide-ranging, routing security in wireless network appears to be nontrivial problem that cannot be solved easily. For enhancement of the various operations in MANET it needs to maintain the appropriate routing information in a distributed manner. Unfortunately there is no such security is considered in routing protocol. Hence there is a need to concentrate on the routing security which plays a significant role in mobile network.

7. REFERENCES

[1] Annapurna P Patil ,Narmada Sambaturu , Krittaya Chunhaviriyakul, "Convergence Time Evaluation of Algorithms in MANETs", International Journal of Computer Science and Information Security(IJCSIS) ,Vol. 5, No. 1,ISSN 1947-5500,PP.144-148, 2009.

[2] Anand Patwardhan, Michaela Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks" , in the Proceedings of the 3rd International Conference on Pervasive Computing and Communications (PerCom), Kauai Island, Hawaii,PP.1-9.2005.

[3] Bo Sun, Kui Wu, Udo W. Pooch, " Routing Anomaly Detection in Mobile Ad Hoc Networks", 0-7803-7945-4/03,IEEE, PP.25-31, 2003.

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

[5] S.Kannan, T.Kalaikumaran,S.Karthik and V.P.Arunachalam, "A Study on Various Attack Detection Methods in Mobile Ad-Hoc Networks", International Journal of Signal System Control and Engineering Application 3(3)ISSN: 1997-5422 published in Medwell Journals,pp.34-39,2010.

[6] Yi-an Huang, Wei Fan,Wenke Lee, Philip S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies", Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS'03) 1063-6927/03, IEEE Computer Society,2003.

[7] Mr. Kamaljit I. Lakhtaria,Mr. Paresh Patel, " Analyzing Zone Routing Protocol in MANET Applying Authentic Parameter", Global Journal of Computer Science and Technology Vol. 10 Issue 4 Ver. 1.0 ,PP.114-118,June 2010.

[8] S.Mangai, A. Tamilarasi, " An Improved Location aided Cluster Based Routing Protocol with Intrusion Detection System In Mobile Ad Hoc Network", Journal of Computer Science 7(4), ISSN 1549-3636, PP. 505-511,2011

[9] Santoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile AdHoc Networks By Dynamic Learning Method", International Journal Of Network Security ,Vol.5, No.3, pp.338-346,Nov,2007.

[10] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, "Different Types Of Attacks On Integrated MANET –Internet Communication", International Journal Of Computer Science and Security (IJCSS) volume (4), Issue (3), PP.265-274, 2010.

[11] Baolin Sun, Hua Chen,Layuan Li, "An Intrusion Detection System for AODV ", Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'05),0-7695-2284-X/05 , IEEE, 2005.