ISSN:0975-9646

MANET: Improved Secured Routing For AODV

Namrata Awasthi
Dept. of Computer Sc. Engg.
RITS, Madhya Pradesh, India

Mr.Anurag Jain
Deptt. of Computer Sc. Engg.
RITS, Madhya Pradesh, India

Mr.Himanshu Yadav
Dept. of Computer Sc. Engg.
RITS, Madhya Pradesh, India

***Abstract*— various routing protocols and techniques are being included in wireless network and making it an area for further research. Congestion avoidance and security are the major areas in Wireless routing which are having research focus. Major research in area of security is focused on key based mechanisms or third party trust management systems. Improved Routing Security is being proposed in this work which will provide the routing protocol security using validating a node for identification which is being distributed to each node through protocol. AODV (Adhoc on Demand Vector) routing is a proactive routing protocol which uses the neighbors' database to find the best route. The work is this paper is focusing on security over routing security and simulations are being proposed to show the improved packet delivery ration, throughput, end to end delay and reduced packet drop rate for Ad hoc On Demand Distance Vector (AODV) routing protocol. Attacks are being avoided proactively by including changes in the basic implementation of AODV routing protocol. Further in this work proposal to provide access control technique and unique key based authentication for AODV is being given. In existing work system performance may affect severely due to application of security mechanisms therefore research scope in this area is always available. Since the industry of communication is growing by leap and bounds therefore the need of continuous research in this area is very much needed.**

***Keywords*— MANET; Identity Based Cryptography; Security; DSDV; Cryptography**

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are technically different from the traditional wireless networks (e.g. wireless LANs, cellular, digital trunked radio or satellite networks). In traditional wireless networks, the fixed network infrastructures such as access points, base stations or satellites are necessarily required to function as the repeaters to relay/retransmit the signal from one node to the others. However, none of these network infrastructures is required in ad hoc networks, that is why ad hoc networks are sometimes called as infrastructure less wireless networks.

Moreover, in traditional wireless networks, data can be transmitted from source to destination within two hops. One hop is required to send data from source to fixed infrastructure, and another from this fixed infrastructure to destination. While data can be sent to destination with one or more hops in ad hoc networks. This means that data can be directly sent to destination by using just one hop if destination is in transmission range of source. However, if it is not in this range, data can be delivered through one or more intermediate nodes until reaching destination. This is simply called multihop communication.

Mobile Adhoc Network (MANET) is a group of mobile nodes which work independently and use radio waves to communicate with each other. Nodes which are nearer and come in the radio range of each other can directly communicate. It provides clear communication & low noise or other disturbing factors are reduced. Whereas, if nodes are far apart from each other than intermediate nodes perform routing to pass the packets to adjacent nodes and deliver to the other end. Distant nodes suffer from problems such as no clear communication, high noise or other disturbing factors etc. These without infrastructure networks are distributed in nature and can work at any place making them extensible and robust in working. [1]

Other important characteristics of these networks are such as wireless communication, nodes performing two roles (hosts and routers), no requirement of centralized controller, dynamic topology and self configuring behaviour etc. These characteristics make them extremely useful in current communication based era and are being applied in almost all areas. MANET is applied in the various fields including the conventional usage areas such as military battlefields, disaster relief efforts, conferences, classrooms, taxicabs, sports stadiums, boats, and small aircraft etc.

As these networks are being applied in various fields, the challenges are also growing to make them free of vulnerabilities being imposed. The major problems being faced in MANET communication are congestion and security. [1]

Initially MANET oriented research efforts were focused on functionality [9]. Nowadays, security is on highest priority since MANETs are being deployed in hostile environments. For achieving security, required services include authentication, confidentiality, integrity, availability, and non-repudiation.

Security measures applied in wired networks are not applicable to MANETs as the characteristics of wireless networks are different due to their "open" network architecture, shared wireless medium, resource constraints, and dynamic network topology impose restrictions for MANETs.[2]

The protocols implemented in ad hoc networks can be roughly classified into two main classes which are proactive (table-driven) and reactive (on-demand) routing protocols. In proactive routing protocols, each node in the network keeps finding the paths to other reachable nodes and inserts them into its own routing table. Note that these paths can be computed based on the routing information which is distributed from the other nodes at predefined interval. In other words, each node periodically maintains and updates its routing table. Hence, each source can immediately send data to destination without waiting for the time required to find a path. However, more routing overhead messages caused by routing advertisement are generated in return which results in some amount of bandwidth consumption.

Whereas the nodes implementing reactive routing protocol find paths to destinations only when they are needed. If source has data to be transmitted, it cannot immediately send the data until path to destination is found. This can be achieved through route discovery process which is occurred on demand. In this process, source sends the route request message in order to either gather the route information or set up the path to destination. Once it receives route reply message, this means that route discovery process is completed and source can start sending the deferred data. This can cause the path set up delay. However, the routing overhead is much reduced due to the fact that the routing overheads including route request and reply messages are flooded only when required by source.

II. Ad Hoc Networking

Ad hoc networks are created instantly as the nodes come in the wireless range of each other. Each node performs the job of host as well as router to provide information to their neighbors. Ad hoc networks can adapt quickly to changes in network topology. Since nodes are movable in the network therefore the changes are very quick in the MANET.

The Ad-hoc On-demand Distance Vector protocol

The Ad-hoc On-demand Distance Vector (AODV) protocol is a suggested protocol for mobile ad hoc networks (MANETs). It is an on-demand, or reactive, routing protocol in its basic configuration. No effort is made to find new routes before a need arises to transmit packets to a destination for which no route exists. The routes are maintained as long as they are needed by existing connections

A. *AODV multicast operation*

The AODV multicast algorithm uses similar RREQ and RREP messages as in unicast operation. The nodes join the multicast group on-demand, and a multicast tree is created in the process. The tree consists of the group members and nodes connected to the group members. This enables a recipient host to join a multicast group even if it is more than one hop away from a multicast group member. The unicast operation of the protocol also benefits from the information that is gathered while discovering routes for multicast traffic. This cuts down the signaling traffic in the network.

B. *Route discovery*

Node performs the step by step processing for discovering the routes between them. Whenever a node wants to find a route from a group, it sends an RREQ message. The destination address in the RREQ message is set to the address of the multicast group.

If the node wants to join the group, i.e., to become a multicast router, the J_flag in the message is set.

Node might respond to a RREQ which is demanding for a route, but only a router in the desired multicast tree may respond to a join RREQ. The corresponding RREP message may travel through nodes that are not members of the multicast group. This means that the eventual route may also include hops through non-member nodes.

The multicast RREP message is slightly different from the unicast RREP. The address of the multicast group leader is stored in a field called Group_Leader_Addr. In addition, there is a field called Mgroup_hop. This field is initialized to zero and it is incremented at each hop along the route. Mgroup_hop contains the distance in hops of the source node to the nearest member of the multicast tree.

C. *Group Hello messages*

Because the protocol relies on a group-wide DSN to ensure fresh routes, the group leader broadcasts periodical Group Hello messages. The Group Hello is an usolicited RREP message that has a TTL greater than the diameter of the network. The message contains extensions that indicate the multicast group addresses and the corresponding sequence numbers of all the groups for which the node is the group leader. The sequence number for each group is incremented each time the Group Hello is broadcast. The Hop_Cnt field in the message is initialized as zero and incremented by the intermediate nodes.

The nodes receiving the Group Hello use the information contained therein to update their request tables. If a node does not have an entry for the advertised multicast group, one is inserted. The hop counts are used to determine the current distance from the group leader.

D. *Multicast tree maintenance*

In a network consisting of mobile nodes, link breakages are bound to happen. The breakages should be repaired promptly to ensure maximal connectivity of the multicast group. Multicast tree maintenance has three different scenarios: activating a link when a new node joins the group, pruning the tree when a node leaves the group, and repairing a broken link. Repairing consists of re-establishing the branches when a link goes down and reconnecting the tree after a possible partition in the network.

In MANET there are various problems due to its open architecture such as access of the wireless channel is available to the eavesdroppers, malicious attackers, legitimate users, hackers etc. Also, there can be defined nodes which will monitor the network traffic or where access control methods can be deployed means there is no clear line of defense can be drawn. Each MANET node functions as router and forwards packets to other peer nodes. Traditional fixed wired networks have dedicated infrastructure such as firewalls, routers, and Intrusion Detection Systems (IDS) to provide protection from outside threats. We can define the difference between the “inside” and “outside” network which may be the way for adding security in the network. Trusted environment is therefore applied by the routing protocols over MANETs, as there is no clear threat to defend against. [3]

III. EXISTING SYSTEM

MANETs were defined by the Defense Advanced Research Projects Agency (DARPA) 1970s when they started with packet radio (PRNET) networks. In this era, Ad Hoc Networks entered a new stage of growth with the popularity and the idea of an infrastructure less wireless network was proposed. With this rapid and sharp growth, problems faced in Ad Hoc Networks have also grown such as problem of congestion, security, self configuration etc. Available protocols are providing solutions to these problems which are not sufficient to cope up with requirements in industries. [15] Major problem anyone views today, is security of communication in MANET, as the application areas of these networks have reached to every part of human lives including banking sector, smart meters etc. Cryptography is used to provide security goals for Ad Hoc Networks because increase threats in network [8]. Shamir proposed the idea of Identity-based cryptography [12]. According to Shamir IBC can enable any two nodes to communicate securely and to verify each other's signatures without exchanging private or public keys, he proposed to calculate public key through his name and network address, while secret key is computed by Private Key Generator which generates key by knowing some secret information that enable it to calculate the secret keys of all users in the network [12]. Boneh and Franklin in 2001 proposed Identity-Based Encryption from the Weil Pairing [14]. They offer a completely practical Identity-Based Encryption scheme (IBE) and provide accurate definitions for secure identity based encryption schemes [10]. Adjih et al in 2005, propose secure OLSR using IBC. All of these and some of the works listed below are having implementing issues such as use of trusted server, inefficiency or providing guaranteed security over the network. [15]

Mobile Certification Authority framework [17] uses specially selected nodes to distribute Certificate Authority (CA). For selecting such nodes it uses security and other physical characteristics of the nodes. Such selected nodes are called MOCA and they provide keys for communication in the network to all the nodes. Such a framework is not good to provide security of the nodes themselves but they provide good security of the data and the users. [16]

Work of Yang [20], is to generate a locally managed token, which is shared with the neighbours for secured communication. Neighbours continuously monitor the node's behavior during routing or packet forwarding services. If the nodes behavior is not good then the token of the node is invalidated, which it can regenerate for future communications. This algorithm termed as Self-organized network layer security (SCAN) is useful in protecting from malicious nodes in the network and do not use any type of encryption for communication. It does not support multipath routing in the ad hoc network. It was proposed for Adhoc On-Demand Distance Vector (AODV) Routing Protocol.

Secure Efficient Ad-hoc Distance (SEAD) [17] Vector routing protocol has suggested one-way hash function to encrypt data and does not use symmetric cryptography operations in the protocol in order to support the nodes of limited processing capabilities. This addresses the problem of sluggish behavior of nodes in Ad-hoc networks and depicts that the nodes in such a network can not behave quick enough to the asymmetric signatures [17]. Since there is no measure employed for grading of the nodes for misbehavior therefore such a protocol is prone to common attacks in MANETs. Security of data delivery is also not available due to missing multipath routing. [17]

A comparative for the work done by various authors has been enlisted in table 1.

IV. PROPOSED WORK

In Manet various nodes come nearby to each other and form a network and therefore security is a primary issue in such networks. Security is to be considered for

Routing Protocol Security

Data Security

IRS – Improved Routing Security is being proposed in this work which will provide the routing protocol security using validating a node for identification which is being distributed to each node through protocol. The overall working of the IRS is as follows:

Step 1: A Network Topology shall be created using NS2 Simulation Environment.

Step 2: Nodes shall be created using AODV protocol routing enabled on them

Step 3: A Pattern Key shall be assigned to each node

Step 4: When a user wants to communicate with the other user then the user will verify the identity and start communication with the other user.

Step 5: For communication Pattern Key of the both the sender and received shall be mixed to make another encryption key and will be used for encryption and decryption of data.

Step 6: Security of the Nodes will impose extra load on nodes and networks therefore we will generate various network response times using different number of nodes in the network.

Step 7: Network throughput, end to end delay, packet drop rate and packet delivery ratios shall be calculated to compare the proposed work with the existing work.

V. SIMULATION ENVIRONMENT

Even though the performance evaluation/analysis of ad hoc routing protocols is usually measured in homogeneous network, this evaluation is not much effective in the real applications where nodes have different capabilities. To study the efficiency and the effectiveness of routing protocols in heterogeneous ad hoc networks, NS-2 simulator [12] is used to construct the simulation. The details of the simulation scenarios and performance metrics are illustrated in the following sections.

Table 1: Comparison between the works of the various authors:

Feature	Rajneesh Agrawal, Sandeep Sahu	Shushan Zhao, Robert D. Kent, Akshai Aggarwal	ZHANG Yong, QIAN Hai-feng	T.H. Lacey*, R.F. Mills, B.E. Mullins, R.A. Raines, M.E. Oxley, S.K. Rogers
Title	Secured Routing Over Manet Using Enhanced Secured Routing (ESR)	An Integrated Key Management and Secure Routing Framework for Mobile Ad-hoc Networks	An efficient identity-based secret key management scheme for MANETs	RIPsec e Using reputation-based multilayer security to protect MANETs
Key Distribution Mechanism	Pattern Key Generated Locally	Trusted Server Based	Top Trusted Dealer, Distributed Private Key Generation	Public & Private Key Certificates
Algorithm Used	Enhanced Secured Routing Protocol for Security during Routing	A Novel Key Management & Security Scheme	simpler threshold version of Schnorr signature (SimpleTSch)	Reputation Based Internet Protocol Security
Multipath	Yes	Yes	Yes	Yes
Problem Taken	Low Performance, Less Security, Congestion & Energy Efficiency	KM-SR interdependency cycle problem, insider attacks, mobile attacks and many routing attacks	Reducing Burdens of Security Management, Efficiency of MANET, Design of Security Protocols for MANET	Attacks in MANET, Network Availability Problem, Encryption, IPSec transport mode, behaviour grading, and multipath routing
Advantages	Uses Local Resources on Nodes, high Efficiency, Low Power Consumption, Less Load on Network, Better Security	Better Security, More Functionality, KM-SR interdependency Removal, efficiency	Better Security, efficiency, Infrastructure Independent, Simple & Easy to deploy	provide an overarching layered security, Protection from external threats & internal threats, End-to-end message security Network availability
Disadvantages	Difficult Pattern Key modification, Security Enhancement	Limited Usage, Security Enhancement, Difficult deployment	Unable to handle security attacks, Low performance	Security of only subsets security challenges, Less Load Efficiency, Adds Extra Load on the Network

A. *Simulation Model*

In heterogeneous ad hoc networks, each node normally has different capabilities since some nodes are portable devices with limited capacity and battery life, while the others may be stationary or equipped with vehicle. These nodes are not power-constrained and usually have higher capacity than the former one. In this research work, there are two types of nodes which are High-capacity nodes (H-nodes) and General capacity nodes (G-nodes). These two types of nodes have different capacity which are bandwidth and transmission range.

Simulation scenarios are constructed by varying number of nodes. In each scenario, a few nodes approximately 5-20% are included as malicious nodes. For example, if there are totally 50 nodes in the heterogeneous networks, 5 nodes of them are the malicious nodes while other nodes are correct nodes performing good communication practices.

TABLE 1: SIMULATION PARAMETERS

channel type	Channel / WirelessChannel
radio-propagation model	Propagation / TwoRayGround
network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
interface queue type	Queue / DropTail / PriQueue
link layer type	LL
antenna model	Antenna / OmniAntenna
routing protocol	AODV
X dimension of the topography	1080
Y dimension of the topography	1080
max packet in ifq	500
seed for random number gen.	0
simulation time	25
number of mobile nodes	500

B. Performance Evaluation Metrics

The performance metrics which are used to analyze the performances of routing protocols in heterogeneous ad hoc networks are discussed in the following:

- Packet delivery ratio (PDR): the ratio of total number of packets received by destinations to total number of packets sent by sources

  ∑ Number of packet receive / ∑ Number of packet send

  The higher value of packet delivery ratio indicates the good performance of the included protocol.

- Throughput is the amount of data in bits received by the recipient. The Mean Throughput is the throughput per unit of duration. network throughput is the rate of delivery of successful messages over a communication line. The throughput is normally evaluated in bits per second (bit/s or bps), and can also be in data packets per second or data packets per time duration.

- Average end-to-end delay: It is the average time needed by a data packet to be available to the recipient. It includes the delay due to route discovery mechanism and the queue in data packet transmission. Only the data packets which successfully reached to destinations are counted.

  ∑ (arrive time –send time) / ∑ Number of connections

  The smaller value of end to end delay indicates the better performance of the protocol.

- Routing overhead: the amount of control data generated/sent to the network by routing protocol

- Packet Drop Rate: the count of packets drop rate for whole of the communication

  Packet lost
  = Number of packet send – Number of packet received
  Packet Drop Rate
  = Average Difference of Packets Received and sent
  The lower value of the packet lost means the better performance of the protocol.

VI. CONCLUSION

The presented work has been intended to provide better security options for the specific MANET which is applicable in a company environment, offices or private networks. Such networks can use the patterned keys to identify their specific nodes and provide better securities over the MANET. Due to the small processing done locally on each node therefore such networks have better performances in respect of the other trust based security mechanisms or symmetric or asymmetric key based mechanisms.

The results obtained from the simulations are encouraging and shows the better security do not affect the performance of the MANET communication. This work can be enhanced in future to provide a dynamic interface to change the key pattern specified so that network can be safeguarded against the human errors.

REFERENCES

[1] Agrawal, R.; Sahu, S., "Secured routing over manet using Enhanced Secured Routing (ESR)," Control Computing Communication & Materials (ICCCCM), 2013 International Conference on , vol., no., pp.1,6, 3-4 Aug. 2013.

[2] Shushan Zhao, Akshai Aggarwal, Richard Frost and Xiaole Bai, “A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks,” IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012.

[3] Y. Zhang, W. Liu, W. Lou and Y. Fang, “Securing mobile ad hoc networks with certificateless public keys,” IEEE Trans. Dependable Secur. Comput., vol. 3, no. 4, pp. 386–399, 2006.

[4] Salaheddin Darwish, Simon J. E. Taylor and Gheorghita Ghinea, “Security Server-Based Architecture for Mobile Ad hoc Networks,” IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 978-0-7695-4745-9, 2012.

[5] Zhao Min, Zhou Jiliu, “Analysis and Improving of Routing Protocols for Mobile Ad Hoc Networks,” IEEE, 978-1-4244-5586-7/10, 2010.

[6] Ahmed. M. Abdel Mo’men, Haitham. S. Hamza and Iman. A. Saroit “A Survey on Security Enhanced Multicast Routing Protocols in Mobile Ad Hoc Networks,” IEEE, 978-1-4244-9924-3, 2010.

[7] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” IEEE Wirel. Commun., vol. 11, no. 1, pp. 38–47, 2004.

[8] Y. Fang, X. Zhu and Y. Zhang, “Securing resource-constrained wireless ad hoc networks,” Wireless Commun., vol. 16, no. 2, pp. 24–29, 2009

[9] Boneh and Franklin, “Identity-based encryption from the weil pairing,” Proc. Crypto 2001, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–219.

[10] J. Marc and N. Gregory, “Identity-Based Cryptography,” IOS Press, ISBN 978-1-58603-947-9, 2009.

[11] T.H. Lacey, R.F. Mills, B.E. Mullins, R.A. Raines, M.E. Oxley and S.K. Rogers, “RIPsec e Using reputation-based multilayer security to protect MANETs,” Elsevier Ltd., 10.1016/j.cose.2011.09.005, 2011.