Dinesh Kumar, D. B. Ojha, Ajay Kumar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 6, November- December 2012, pp.884-889

Securing MANETs by Q Routing Protocol

Dinesh Kumar[*1], D. B. Ojha[2], Ajay Kumar[3]

*[1]Department of Computer Science , Mewar University., Chittorgarh, Rajasthan, INDIA ji.dinesh@gmail.com[1]
[2]Department of Mathematics, Mewar University., Chittorgarh, Rajasthan, INDIA ojhdb@yahoo.co.in[2]
[3]Department of Computer Science , Mewar University., Chittorgarh, Rajasthan, INDIA ajaycpp@gmail.com[3]

Abstract

MANETs is a infrastructure less network in which all the nodes are move independently so there are lot of chance for unsecure the network..for securing the adhoc network we have different-different routing protocols such as AODV, DSR, OLSR, SAR , SRP and Ariadne. And to allow comparison of these secure protocol there is a single common routing protocol i.e. Q Routing. Our contribution in this work to develop a secure and comprehensive network. Q Routing is a adaptive routing protocol which provides the alternate path between the routing nodes in the condition of when the route is fail.

Keywords: MANETs, AODV, DSR, OLSR, SAR, SRP, Ariadne, Security.

Introduction

Generally all the device are communicated in the fixed infrastructure or centralized infrastructure so if we want to connect devices in the independent manner so that they can communicated well so for that purpose we establish the Adhoc network to gather so that all devices are smoothly connected in systematic manner.

A mobile ad hoc network or also called as a *wireless ad hoc network* is a wireless network,in which all the device use wireless transmission for communication without any fixed or centralized infrastructure. Such as a base station in cellular network or an access point in wireless local area network. all the nodes are free to move randomly and organize themselves arbitrarily so due to this wireless topology change time to time. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Unlike traditional mobile wireless networks, mobile ad hoc networks do not depend on any central coordinator but communicate in a self organized way.

In general, a wireless node can be computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, or a animal, or an airplane, to enable wireless communication among them.Information exchange in a network of mobile and wireless nodes without any infrastructural support.Such networks are often called ad hoc networks. Adhoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information among the several nodes which are exist its environment. Wireless nodes can be personal computers or it can be desktop or laptop with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices.

MANET's network is useful in the field of army, classroom study, and collaborating and distributed computing.

1.1 Advantages of MANETs

There are so many advantages of MANETs such as-

Required Less Cost for installation:- For deploying the Ad hoc networks there is very less cost is required such as copper wires or data cables.

Easy to access: - Each node is free to communicate among all nodes independently without any fear but there is lack of trust is required.

Fast deployment: - In a very short period of time Ad hoc networks can be deployed without any cable involved.

Dynamic Configuration: - Adhoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

1.2 Applications on MANETs

Now a days there are so many applications in MANETs such as:- Military applications, such as providing communication among a team of soldiers for different operations when setting up a fixed wireless communication infrastructure in enemy territories or in inhospitable terrains may not be possible. Emergency systems, for example, establishing communication among rescue personnel in disaster-affected area that need quick deployment of a network. Commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture Collaborative and distributed computing. Wireless mess networks and wireless sensor networks.

In MANET, a wireless node can be the source, the destination, or an intermediate node of data

transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbour closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. so the network topology changes from time to time.

Problem in MANETs

The main problem in MANETs is that MANETs do not have a fixed infrastructure and may not have constant access to the Internet central authorities. As a result, the existing security services embedded in the internet may not be available to MANET applications. Generally there are three types of problem in MANETs these are trusted communication and trusted identity, trusted application,

1.3.1 Trusted Communication in MANETs

Due to the lack of infrastructure, a node can potentially establish a direct connection with another node by roaming into its wireless signal range, which by passes any pre-deployed choke points. A more general issue than protecting nodes from being attacked by their network peers is how to assure secure communication and proper collaboration among all participant entities. This is important especially for spontaneously formed MANETs, Moreover, in client server applications, the goal of application communication policy is usually server-centric, meaning that it aims at protecting the server from unauthorized access from the client.

1.3.2 Trusted Identity in MANETs

Generally in MANET all nodes are moves frequently so if any one node sends message to another node so there is lot of chance to damage the message because we can identify which node sends the packet. So authenticating a node can be further reduced to the problem of authenticating the node's public key. In the infrastructure based networks, the public key can be sealed in a digital certificate signed by a third-party i.e. certificate authority (CA). so C A verify the certificate with the CA, the public key is authenticated.

1.3.3 Trusted Application in MANETs

There are many applications run independently in infrastructure based or infrastructure less network so it is very typical to identify the particular applications suppose in client server architecture the client and server applications running in infrastructure based network so there is necessary to maintain the trust between the client and server. so the client and server provide the relationship among the business companies**.** For a client in client-server applications running in infrastructure based networks, the trustworthiness of the server application itself is usually of little concern. More attention is paid to ensure the trustworthiness of the server's owner.

2. MANET Routing Protocol

In a network if one node sends message to another node which it cannot reach properly so for that purpose we have AODV and DSR protocol so it send the message to its neighbouring nodes which it cannot directly communicated.

AODV and DSR are the most popular on-demand protocols. they enable nodes on the network to pass messages, via their neighbours, to nodes with which they cannot directly communicate. This is achieved by discovering routes along which messages can be passed and they ensure that these routes are devoid of loops and try to find the shortest possible path. Further, they are also able to handle changes in routes and can create new routes if there is an error or change in topology, which is a very important requirement for routing in MANETs.

2.1 Secure Routing Protocol (SRP)

Secure Routing Protocol provides the guarantee the acquisition of accurate topological information and also that a node initiating the route discovery process would be able to discard replies from malicious nodes which are claiming false topological information, thus it provides maximum safety. Although it prevents the black hole attack and also the attacks due to incorrect routing information, SRP does not solve the problem of protecting transmitted data but it handled by the Secure Message Transmission Protocol.

2.2 Security-Aware Ad hoc Routing (SAR)

SAR is just used to discover routes efficiently. Though, it is unable to clearly state how to use it as such SAR prevents a few attacks such as spoofing and the black hole attack among others or It provides the generalized way of providing security to routing protocols.

2.3 Authenticated Routing for Ad hoc Networks (ARAN)

It is a secure routing protocol based on the on-demand protocols. It is used to assign the digital certificate to every node so that they can be identify the every node in the network. Generally it is use asymmetric cryptography and there is third party i.e. (DCA) digital certification authority (CA) which assigns a digital certificate to every node on the network. There are five major parts in ARAN those are- Discovery, Certification, Route Maintenance, Authenticated Route and Key Revocation. All nodes that want to enter the network must request a certificate from the CA. if any node want to send message to other node so first of all it starts the communication by sending the route discovery packet and the target node replies

with an route request packets to the initiator, where it is verified. Every node on any particular route that receives a route request strips the signature and certificate of the previous node and appends its own into the packet before sending it to other node.

2.4 Secure Adhoc On Demand Distance Vector Routing (SAODV)

There are two method such as route requests and route replies are authenticated to guarantee their integrity and authenticity. The source node signs the routing message with its private key, and the recipient nodes verify the signature using the public key of the source node. So hop count must be incremented at each hop, the sender is unable to sign it. If there is need some modification in intermediate node so there is hash chain mechanism is used to prevent any modification or tampering of the hop count by hostile intermediate nodes. In SAODV, an RREQ packet includes a route request single signature extension (RREQ-SSE). An upper bound for the hop count is chosen by the source node and it generates a one-way hash chain. The length of this one-way hash chain equals the maximum hop count incremented by one. The route request and the anchor of this hash chain are both signed by the source node and both are included in the RREQ single signature extension (RREQ-SSE).

2.5 ARIADNE

It is a robust protocol based on Dynamic Source Routing that has been used broadcast authentication technology. Ariadne makes use of symmetric key cryptography. It also uses a one way hash along with a MAC using a shared key between the source and the destination.

3. Security Aspects in MANETS

The ultimate goals for MANETs is to provide security services, such as authentication, integrity, confidentiality but there are common security services which are as follow.

3.1 Availability

Availability provides the continuity to the service despite of various attacks. It maintain the serviceability throughout the network. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network.

3.2 Integrity

Integrity ensure the registration of the authorized party so that they can only allowed to modify the information or message**.** Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that when the message is being transmitted it will never corrupt. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays.

3.3 Confidentiality

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality.

3.4 Nonrepudiation

Generally norepudiation is useful for detection and isolation of compromised nodes. Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver.

3.5 Authentication

By authentication only valid parties are having right to access and supply the message from one node to other node**.** It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning signal or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without authentication, an Security Services adversary could discard the node so gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes.

3.6 Scalability

Scalability is the important factor in security services and it is not directly related to security
it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system.

4 Security Attacks in MANETs

There are two types of Attacks such as passive attacks and active attacks.

Passive attacks: A passive attack does not disrupt the normal operation of the network, in this detection of the passive attack is very difficult so the detection of the network is get affected.. Attacker snoops the data exchanged in the network without altering it. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted.

Active attacks: An active attack attempts to alter to destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network.

4.1 Attacks Using Fabrication

In this the intruder generates false routing messages, such as routing updates and route error messages, in order to disturb network operation or to consume other node resources. A number of fabrication based attacks are presented below

4.1.1 Resource Consumption Attack

In this type of attack a malicious node deliberately tries to consume the resource such as battery power, bandwidth, etc of other nodes in the network. The attacks could be in the form of unnecessary route request control message or forwarding of stale information to nodes.

4.1.2 Rushing Attack

On demand routing protocols that use route discovery process are vulnerable to this type of attack. An attacker node which receives a "route request" packet from the source node sends the packet quickly throughout the network before other nodes which also receive the same "route request" packet can react.

4.1.3. Black hole attack

In this type of attack, a malicious node falsely advertises good path such as shortest path to the destination node during the path impersonation. such as masquerading or spoofing , modification, fabrication and replication. Both passive and active attacks can be made on any layer of the network protocol stack.

4.1.4 Gray hole attack

The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly.

5 Preliminaries

All the routing protocols are work in OSI model under the frame of data link layer and network layer. In data link layer there is one hop connectivity and frame transition. But in network layer there is routing and data packets forwarding [Zhou and Haas(1999), Komninos, Vergados and ouligeris(2007), Kong(2002)]. Data link layer protocols provide the connections between neighbouring nodes and will also provide the accuracy of the transmitted frames. As routing protocols exchange routing data between nodes, as a result, they would maintain routing states in each node. Based on routing states, data packets are transmitted by mediated nodes along an established route to the destination. The detection procedure, tried to detect the unauthorized nodes. This phase of our scheme is based on Komninos and et al.'s framework and use a non-interactive zero knowledge technique [Komninos, Vergados and ouligeris(2007).

Q -Routing [Boyan & Littman (1994)] is an adaptive packet routing protocol for static networks based on the Q -learning works. It is essentially a version of the distributed Bellman-Ford algorithm. The algorithm allows a network to continuously adapt to congestion or link failure by choosing routes that require the least delivery time. When a route becomes congested or fails, Q -routing learns to avoid that route and uses an alternate path. Due to its adaptive nature, we might expect that Q -routing would also work well in the mobile ad-hoc setting. Q -routing is a direct application of Watkins' Q learning [Watkins (1989)] to the packet routing problem. Each node in the network runs its own copy of the Q -routing algorithm. A node x faces the task of choosing the next hop for a packet destined for some receiver node d . Using Q-routing, it learns the expected delivery times to d for each possible next hop y , where each possible next hop y is a neighbor node connected to x by a network link. Formally, Q -routing keeps Q -tables Q_x for each node x and updates these tables at each time period t as follows:

$\boldsymbol{Q_s^a}$ **(m, b) =** $\boldsymbol{\alpha(y_s^a + min_c\ Q_{s-1}^b}$ **(m, c)) + (1 -** $\boldsymbol{\alpha)\ Q_{s-1}^a}$ **(m, b)** where $\boldsymbol{0<\alpha<1}$ is parameter that controls the learning rate, here ys is the time where current packet is spent on the buffer at node a. and s is the time spent period.and U is the estimated cost which are bouded each state m with U.

so U = $min_c\ Q^a$ (m,c) [y chang T ho and LP Kaelbling (2003)] is the value of a state is the estimated time for a delivery a packet from the

currunt node a to destination node m via node c. when the nodes are once analyzed then the value associated with each state- action pair so they simply adopt the greedy policy. When a node receive a packet for destination m. so before sending the packet to it. It sends the packet to its neighboring nodes b with the lowest estimated deliver time Q^a (m,b) and neighbor node are defined as the node with in the transmission range. So there are main difference is the neighbor node b may appear or disappear quite frequently due to node mobility.

When node b moves out of range we set the estimated delivery time to m via b to ∞. i.e. Q^a (m, b) $= \infty$

When node b moves into range we optimistically bias encourage exploration. i.e. node a will always try to sending packets via a node b which are belong to its range. But in the case of high delivery estimated time then node a will quickly revert to its original behavior. Since Q^a (m, b) will be updated in short period to its estimated value otherwise nod a will send packets via node b for a good delivery time.

6 Result

let us consider M_{first} and M_{second} nodes are verified when node x1 enter in the MANETs.so after that its authentication is done by neighboring nodes m first and m second, so there is new route will be created between nodes.When the node x1 is verified as a valid node in the MANET. So routing and transmitting packets would be done through them. In wireless environments there is not interactive zero protocol and not suitable because they exchange many message and this case network efficiency will be decrease so there are non interactive zero knowledge protocol are suitable for MANET.

In this the node do not need to exchange message to verify their identity to the nodes m first and m second. and generate that discrete logarithm of $p_1 = x^{m1}$ and $p_2 = y^{m2}$ with base x and y.

7Implementation

After convincing that discrete logarithms build linear equation to m first and m second so that there is equation: $e_{m1} + f_{m2}$ = U (mod l) where e, f, l are integers and l is a large prime number. And u is the constant cost. and m_1 and m_2 are two time interval so after that we calculate the equation p_3 = r m_3 and p_4 = i m_4 and solve e m_3 + f m_4 = o(mod l) and after that message send to m first by node x_1 is p_5 = xm_3 and for node x_2 the message is p_6 = ym_4 so we apply hash function by m first and m second to x_1 i.e.

p_7 = H(x, y, e, f, u, p_1, p_2, p_5, w_6) and applying some validation of p_5 p_6 by x_1 again we get message p_8 = m_3− p_7 m1(mod l) for m_{first} and p_9 = m_4 − p_7 m_2 (mod l) for m_{second} and that calculate M_{first} and M_{second} p_{10} = x^{p8} p_1^{p7} , p_{11} = x^{p9} p_2^{p7} and p_{12} = H(x,y,e,f,u, p_1, p_2, p_{10}, p_{11}) and e p_8 + f p_9 and p_7 u(mod l) so after analysis M_{first} and M_{second} if $p_8 \neq p_4$ and $p_9 \neq p_5$ so $p_{10} \neq p_6$ so x_1 is not reliable and if ep_5 + fp_6 ≠ p_4u(mod l) so the identity of x_1 is not authorized.

8 Conclusions

In this article we provide descriptions of several routing schemes proposed for ad hoc mobile networks. We provide a classification of these schemes according to the routing strategy (i.e., table-driven and on-demand). The field of ad-hoc mobile networks is rapidly growing and changing, and while there are still many challenges that need to be met, it is likely that such networks will see widespread use within the next few years.

Q Routing is the protocol which providing new route when the route is fail between the routing node in MANET and it also explains how to make optimal decision for solving the routing problem and it is also useful to finding the optimum route and recognizes the unauthorized intruder in MANET.

We have discussed security issues related to integrated mobile ad hoc network (MANET)-Internet and stand alone MANET. The proposed mechanisms until now have solved many security issues related to integrated MANET-Internet communication but they have not solved them completely. So, we can design a security mechanism by which we can minimize or completely remove many of those attacks.

In future, we will propose to design a robust framework that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security. The performance analysis of the protocol shall be done using NS-2 simulation software. It is expected that it shall minimize the security attacks due to both integrated MANET-Internet and stand alone MANET.

References

[1] J. Kong, Adaptive Security for Multi-layer Adhoc Networks, Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press, 2002.

[2] Y. Chang, T. Ho and LP. Kaelbling, Multi-agent learning in mobilized ad-hoc networks, AI Lab Memo, AIM-2003-025, 2003.

[3] Boyan, J., and Littman, M. L. 1994. Packet routing in dynamically changing networks: A reinforcement learning approach. In Advances in NIPS.
[4] Watkins, C. J. 1989. Learning with delayed rewards. Ph.D. Thesis, University of Cambridge.
[5] P. Brutch and C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, The Symposium on Applications and the Internet Workshop, 2003, 368-373.
[6] D.B. Johnson and D.A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, *Mobile Computing*, chapter 5, pp. 153-181, (Kluwer Academic Publishers, 1996)
[7] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, Ad hoc On-Demand Distance Vector (AODV) Routing.
[8] RFC 3561, Jul 2003. Luke Klein-Berndt *A Quick Guide to AODV Routing*, National Institute of Standards and Technology, US Department of Commerce, USA.Available on: http://w3.antd.nist.gov/wctg/aodv_kernel/aodv_guid e.pdf/
[9] Y. C. Hu, D. B. Johnson, and A. Perrig, SEAD:Secure efficient distance vector routing for mobile *Elsevier, Vol. 1, Issue 1*, July 2003, Pages 175–192.
[10] M. Guerrero Zapata and N. Asokan, Securing Adhoc Routing Protocols, in *Proceedings of the 1stACM workshop on Wireless security*, Atlanta, GA, USA, Sep 2002, pp. 1–10
[11] P. Ramachandran and A. Yasinsac, Limitations of On Demand Secure Routing Protocols, *IEEE Information Assurance Workshop 2004*, June 10-11, 2004, pp. 52-59
[12] S. A. Ade; P.A.Tijare, (2010). "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks." July-December 2010, Volume 2, No. 2, pp. 545-548.
[13] Huseyin Arslan, Zhi Ning Chen and Maria-Gabriella DiBenedetoo (eds) – " Chapter 15 – An Overview of Routing Protocols for Mobile Ad Hoc Networks – Ultra Wideband Wireless Communication" – John Wiley and Sons, 2006.
[14] H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hoc networks,*" Cincinnati Univ., OH,USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

Dinesh Kumar [M. Tech (P), MCA, B. Sc (Physics, Math.)]
Dinesh Kumar is an Assistant Professor in Department of Computer Science and Information Technology at Mewar University, Chittorgarh (Rajasthan). He has Completed B. Sc (Physics, Math.) from CCS University, Meerut, U.P. and Completed MCA from U. P. Technical University, Lucknow and M. Tech(P) at Mewar University, Chittorgarh (Rajasthan).

Specialization:
Mobile computing, DBMS, Programming language, Design and analysis of algorithm, Computer networks.