IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Analysis of Security Issues In Reactive Routing Protocols.

Ravinder Kr. Gautam[*1], Shikha Jain[2], Lakshman Das[3], Sunil Kumar[4], Rohit Tanwar[5]
*1,3HIET Ghaziabad.
[2]Amity Noida.
[4,5]MRCE Faridabad.
rkrgautam@gmail.com

Abstract

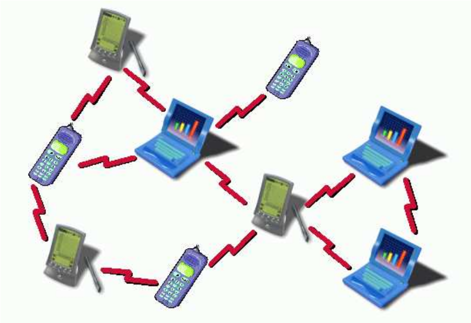
The field of mobile computing can be described as both old and new. Today with the popularity of new generation mobile devices, the focus is moving towards the mobile based: - user experience, next generation solutions, cloud services and infrastructure. Therefore, we can say that ad-hoc network is an emerging area of mobile computing. In comparison to the wired networks, mobile ad hoc networks have unique characteristics. But these features results in a number of significant threats to the security design, such as open peer-to-peer network architecture, shared wireless medium, confined resource constraints, and dynamic network topology. So, ad-hoc networks throw up new requirements and problems in all areas of networking .Now the situation demands a solution comprising of basic security components (prevention, detection, and reaction) .The objective of the included components should enhance the security of system .The end result of the solution must ensure the properties like authentication, confidentiality, non-repudiation, integrity, and availability. This paper provides the descriptive details of the routing protocol DSR with its security issues. Firstly, we attempt to analyze the security requirements concerning the ad hoc network .Secondly, the detailed explanation of the routing protocols are mentioned. Lastly, comparison of these protocols is done on the basis of providing security against the various network attacks.

Keywords: Routing Protocol, DSR, Manet.

Introduction

A mobile ad-hoc network (MANET) can be defined as a self-configuring network including the mobile hosts equipped with wireless communication devices. The unique features are: working without a central coordinator, multi-hop radio relaying, and frequent link breakage due to mobile nodes, constraint resources and instant deployment. In an ad hoc network, no base stations or mobile switching centers are present. Mobile nodes that are within each other's radio range communicate directly by wireless links, while those that are far apart rely on other nodes to relay messages as routers. Therefore, we can say that node mobility causes frequent changes in the network topology.

The salient features of ad hoc networks pose several security related challenges. Firstly, usage of wireless links makes an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation. These types of attacks may result in the loss of confidential information, alteration of secret messages, violation of authentication and non-repudiation. Secondly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership. Thirdly, the lack of an online CA or Trusted Third Party adds the problem of deploying the required security mechanisms. Finally, mobile devices do have limited power consumption and computation capabilities .This limitation makes it susceptible to some attacks and incapable in executing algorithms.



igure 1**:** An Ad hoc Network

We can safely conclude that the mobile ad hoc network is not secure as nodes are free to join, leave and move inside the network. So it is quite possible that few nodes may be compromised by the adversary and thus performs malicious activities which are difficult to detect.

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. This protocol allows the network to be self-organizing and self-configuring in nature. As it includes two mechanisms named as route discovery and route maintenance respectively.

Literature Review

Dynamic Source Routing was proposed by Broch, Johnson, and Maltz [6] for the MANET. This protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. Many research scholars had done significant work in the field of MANET.

Zhou and Haas [8] focused on the key management aspect. They described the concept of secure routing and finally concluded that “nodes can protect routing information in the same way they protect data traffic”. They also observe that denial-of-service attacks against routing will be treated as damage and routed around.

S. Marti, T. J. Giuli [4] worked as to secure ad hoc networks by using misbehavior detection schemes. There approach had two major flaws :(i) it is quite likely that it will be not feasible to detect several kinds of misbehaving (especially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures); (ii)has no real means to guarantee the integrity and authentication of the routing messages will not be violated.

ARAN was proposed by Kimaya Sanzgiri et al [1] .It is a routing protocol used in ad hoc networks. Its basic requirement is trusted certificate server. Each node sign both the messages (route discovery or a route reply message).But, this result in increased size of the routing messages. This protocol is not immune to the reply attacks.

Hubaux, et al introduced the concept of equal participation of the ad hoc group members. The participation provides the rights to node for issuing the certificates [3].Kong; et al. [5] has proposed a secure routing protocol based on secret sharing. But there is one issue with this protocol, as it is based on erroneous assumptions, e.g., that each node cannot impersonate the MAC address of multiple other nodes.

Ariadne [2] is based on DSR [6] and the authentication mechanism called as TESLA .S. Buchegger, and J.-Y. Le Boudec [7] proposed CONFIDANT routing protocol .It is an extension of DSR to provide security.

Categories of Manet Routing Protocol

In mobile ad hoc networks, the protocols are used for the routing of nodes. These protocols are classified as:-

- Proactive routing protocols
- Reactive routing protocols

A reactive routing protocol tries to find a route from S (source) to D (destination) only on-demand, i.e., when the route is required, for example, DSR and AODV are such protocols. The main advantage of a reactive protocol is the low overhead of control messages. However, high latency in discovering routes is the major issue in reactive protocols. Whereas in proactive protocols, complex and detailed routing tables are maintained for the complete network. So, we can say route discovery is an easy process in proactive protocols. Therefore, it’s its low latency in discovering new routes are the main advantage. But, in order to update the status of table, this protocol generates a high volume of control messages.

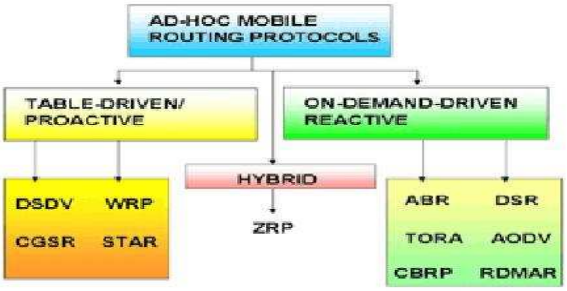


Figure 2: Types of routing protocol

Routing in an ad-hoc network depends on many factors like network topology, selection of routers, initiation of request etc. There is a need of optimal routing, due to low resource availability. The highly dynamic topology of these networks imposes several challenges to the routing protocols specifically designed for them.

Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol uses the source routing approach i.e. (every data packet carries the whole path information in its header) to forward packets. Before a source node sends data packets, it must know the total path to the destination. Otherwise, it will initiate a route discovery phase by flooding a Route Request (RREQ) message. The RREQ message carries the sequence of hops it passed through in the message header. Any nodes that have received the same RREQ message will not broadcast it again. Once an RREQ message reaches the destination node, the destination node will reply with a Route Reply (RREP) packet to the source. The RREP packet will carry the path information obtained from the RREQ packet. When the RREP packet traverses backward to the source, the source and all traversed nodes will know the route to the destination. Each node uses a route cache to record the complete route to desired destinations. Route failure is detected by the failure of message transmissions. Such a failure will initiate a route error message to the source. When the source and the intermediate nodes receive the error message, they will erase all the paths that use the broken link from their route cache.

Pros

- The path calculated in DSR is loop-free since loops can be detected easily and erased by the source routing.
- It is simple and loop-free.
- Routes maintained only between nodes that needs to communicate.
  -- reduces overhead of route maintenance.
- Route caching can further reduce route discovery overhead.
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

Cons

- The response time may be large since the source node must wait for a successful RREP if no routing information to the intended destination is available.
- In addition, if the destination is unreachable from the source node due to a network partition, the source node will continue to send RREQ messages, possibly congesting the network.
- Packet header size grows with route length due to source routing.
- Route Reply Storm problem

Security Requirement of AD HOC Network

In order to solve the security issues of an ad-hoc network, security requirements needs to be accomplished. The brief explanations of the requirements are: -- integrity, confidentiality, availability, authentication, non-repudiation, dependability, reliability, accountability. As there are so many threats to protect from, therefore there can't be a general solution. Different applications have different security needs. Therefore, as a result of this diversity, various approaches have been introduced focusing on different kinds of the problem.

Exploits allowed by DSR routing Protocol

A) Attacks Using Modification

The malicious nodes tend to forward the messages with false values or change the message fields so that network is congested. This congestion degrades the network performance and violates the integrity of the data. These malicious nodes may alter the source routes so as to result in the denial of service attacks.

B) Attacks Using Impersonation

These attacks are called spoofing since the malicious node hide its real IP address or MAC address and uses another one. As current ad-hoc routing protocols like DSR do not authenticate source IP address, a mailicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take Ip address of other node in the network and then use them to announce new route to the other nodes. By doing this, he can easily modify the network topology as he wants.

C) Attacks using fabrication

The generation of false routing messages can be classified as fabrication attacks. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted. Falsifying routes and route cache poisoning attacks in DSR.

Attack	AODV	DSR
Remote Redirection		
➢ Modification of sequence numbers	✓	✗
➢ Modification of hop counts	✓	✗
➢ Modification of source routes	✗	✓
➢ Tunneling	✓	✓
Spoofing	✓	✓
Fabrication		
➢ fabrication of error messages	✓	✓
➢ fabrication of source routes	✗	✓

Table 1. Vulnerabilities of AODV and DSR

Security Routing in AD HOC Network

There exist several proposals that attempt to architect a secure routing protocol for ad hoc networks, in order to offer protection against the attacks mentioned in the previous section. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing ones (like DSR). As we will see, the design of these solutions focuses on providing countermeasures against specific attacks, or sets of attacks. The following routing protocols are extension to DSR to provide security.

1) SRP (Secure Routing protocol)

It is applicable on many existing protocols like DSR .In this, a security association (SA) is established between the source and the destination node. In order to establish a secure channel a secret symmetric key is exchanged between the nodes. Then, the SA verifies whether the participating node is trusted or malicious. The route discovery is started by source node by the transmission of Route Request packet (RREQ).Then, calculation of the Message Authentication Code (MAC) is performed by source and destination nodes using the unique query identifiers. RREQ packets also include the addresses of the traversed intermediate nodes. The intermediate nodes transmit RREQ packets so that one or more query packets arrive at the destination. Route reply packet (RREP) is created once the RREQ packet reaches the destination. MAC is calculated and packet is return to source over the reverse route of RREQ.

The properties of SRP:-

- Combating against the route discovery process
- Detecting and discarding bogus replies
- Immune to IP spoofing, etc.

Limitations

- Not immune to wormhole attack
- Suffers from route cache poisoning
- Lack of a validation mechanism for route maintenance messages.

2) CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks)

This protocol works as an extension to a reactive source-routing protocol for mobile ad-hoc networks. It was proposed by S. Buchegger, and J.-Y. Le Boudec [8].Selective altruism and utilitarianism forms the basis of this protocol. Detecting and isolating misbehaving nodes is the main focus. Its components are:- monitor, reputation system, path manager and trust manager. These components are present in every node. The path manager is connected to the routing protocol, DSR for the specification. The monitor component manages the DSR specifications verification like packet forwarding. The monitor component calls the trust manager and reputation system if there is a mismatch between verification and specification.

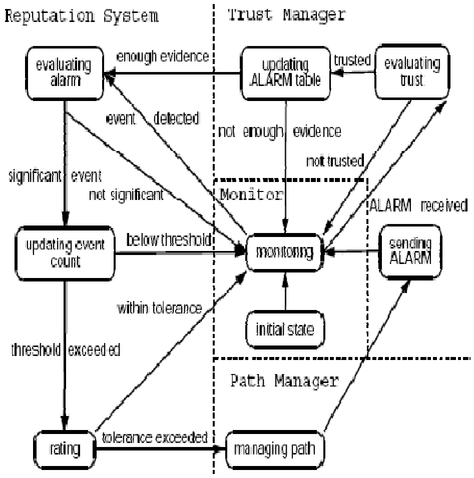


Figure 3: Working of Confidant Protocol

3) ARIDANE

It is an on-demand secure routing protocol based on DSR. It depends on symmetric cryptography. It was proposed by Y. C. Hu, A. Perrig, and D. Johnson [2]. The security of
Aridane depends on the secrecy and authenticity of keys stored in nodes.

The following keys are used:-

- If pair wise shared secret keys are used, we assume a mechanism to set up the necessary n(n+1)/2 keys in a network with n nodes.
- If TESLA is used, we assume a mechanism to set up shared secret keys between communicating nodes, and to distribute one authentic public TESLA key for each node.
- If digital signatures are used, we assume a mechanism distribute one authentic public key for each node.

It works in two stages. In the first stage, the authenticities of RREQ packets are checked. In the next stage, it is verified that no node is missing from the node list by using per-hop hashing technique. Message authentication code (MAC) is present in the source node. Shared key is used to verify the RREQ authenticity and freshness by the intermediate as well destination nodes. This checking is required, so that destination node can send a RREP packet.

Features are highlighted as below:

- Handles nodes that can modify/ fabricate routing information
- Combats against attacks such as impersonation, wormhole
- Copes against compromised nodes; RREQ flooding is avoided.

Limitation:-

- Need of clock synchronization between the participating nodes.

Protocols	Attacks				
	Black hole	Replay	Wormhole	DoS	Routing table poisoning
ARIDANE	✗	✓	✗	✓	✓
SAR	✗	✓	✗	✓	✓
CONFIDANT	✓	✓	✗	✗	✗

Conclusion

Secure routing is one of the most basic task and major concern as well in a MANET. Many protocols have been proposed but still they do not provide full security. In this paper, we highlight the security requirements, security issues, routing protocols like DSR and extensions of DSR. That's why we decided to use the formal verification technique on DSR in relation to its security properties. It is possible to showcase the behavior of protocols using the simulators. But even they fail to ensure the security features of a network. This technique assures a system has, or has not, a given property.

References

[1] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02), IEEE Press, 2002, pp. 78-87.

[2] Y. C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Technical Report TR01-383, Rice University, Dec. 2001.

[3] J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In Proc. ACM MOBICOM, Oct. 2001.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.

[5] J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

[6] Dave B. Johnson and David A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, October 1999.

[7] S. Buchegger, and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)," Proc. 3rd Symp. Mobile Ad hoc Networking and Computing (MobiHoc 2002), ACM Press, 2002, pp. 226-236

[8] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24–30, November/December 1999.