International Journal of Advanced Education and Research
ISSN: 2455-5746, Impact Factor: RJIF 5.34
www.newresearchjournal.com/education
Volume 1; Issue 2; February 2016; Page No. 48-51

Security and adaptability of routing in wireless network

Meenu Kamboj

Department of Computer Science, Kurukshetra University, Kurukshetra, Haryana, India

Abstract
Security is an essential service for wired and wireless network communications. It is very challenging for researchers to provide comprehensive security for wireless moving networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper, we review different protocols with a particular focus on security aspects. Secure wireless moving networks have to meet five security requirements: confidentiality, integrity, authentication, non-repudiation and availability. The analyses of the secure versions of the proposed protocols are discussed with respect to the availability and security of routing in wireless moving network. In the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In this paper, we examine routing attacks, such as link spoofing and colluding miserly attacks, as well as countermeasures against such attacks in existing MANET protocols. The proposed Scheme will take care to evaluate various security designs and to implement in existing protocols. Efforts will be made to make wireless moving networks data transfer reliable. Algorithm will be developed to achieve stable data transfer. Finally effort will be made to merge the existing scheme with new scheme to get better scalable design.

Keywords: wireless moving network, security, routing

1. Introduction

A Wireless Moving Network (WMN) is an emerging technology that has been attracting tremendous attention from researchers. Because these networks can be deployed quickly without relying on a predefined infrastructure, they can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces.

A Wireless Moving Network (WMN) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a WMN is free to move independently in any direction, and will therefore change its links to other devices frequently. The main challenge in building a WMN is maintaining each device to continuously maintain the information required for proper routing of traffic. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

For example, A VANET (Vehicular Wireless Network) is a type of WMN that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet.

The backbone of the wireless moving network is routing**.** Routing is the process of forwarding packets from source to destination using most efficient route. Efficiency of the path/route is measured in various metric like number of hops, traffic, security etc. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency. All WMN routing protocols could be broadly classified into three major categories: Pro-active Routing Protocols, Reactive Routing Protocols, and Pro-active Routing Protocols.

1.1 Types of wireless moving Routing Protocols

1) **Proactive routing protocol**: In proactive routing scheme every node continuously maintains complete routing information of the network. This information is stored in tables. Each node maintains a routing table which contains the list of destinations and routes
2) **Reactive routing protocol**: The reactive routing protocols are based on some sort of query-reply dialog. In this the nodes do not need periodic transmission of topological information of the network. When there is a need for a route to a destination, route request messages are flooded periodically with new networks status information. Every node in this routing protocol maintains information of only active paths to the destination nodes.
3) **Hybrid Routing Protocols**: Often reactive or proactive feature of a particular routing protocol might not be enough. These protocols combined the features of both reactive and proactive routing protocols. Figure1 is description of popular routing schemes

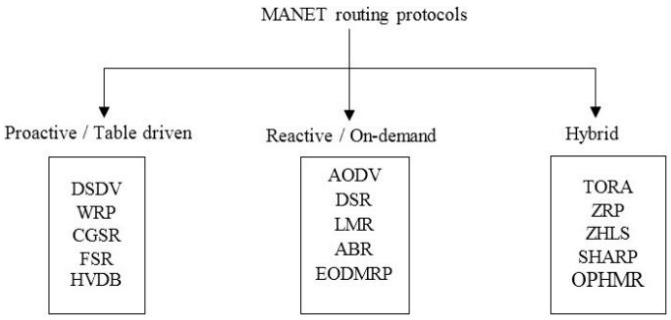

Fig 1: Routing Protocols

2. Security Issues

Security of WMNs is major deployment concern. Due to the mobility and wireless nature of the network malicious nodes can enter the network at any time, the security of the nodes and the data transmitted needs to be considered [1]. The main goal of the security solutions for a Wireless network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [2]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in a wireless network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. The prime concern is with the attacks targeting the routing protocols for Wireless Networks. These attacks [3, 4, 5, and 6] can be broadly classified into two main categories as: Passive attacks, Active attacks

2.1 Types of Attacks

1) Passive attacks*:* In a passive attack an unauthorized node continuously monitors the network and willing to get the information. In this the communications is not interrupted. There is no direct damage to the network. The attacker can read the information which can be used for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

2) Active Attacks: These attacks cause unauthorized state changes in the network such as denial of service, modification of packets etc. These attacks are generally launched by users or nodes with authorization to operate within the network. The active attacks can be classified into four groups: dropping, modification, fabrication, and timing attacks. An attack can be classified into more than one group.

2.2 Attacks against Wireless Moving Networks

Flooding Attack

The aim of the flooding attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. A flooding attack can decrease throughput by 84 percent.

Black hole Attack

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure 2 shows an example of a black hole attack, where attacker 3 sends a fake RREP to the source node 1, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node 1 will choose the route that passes through node 3.

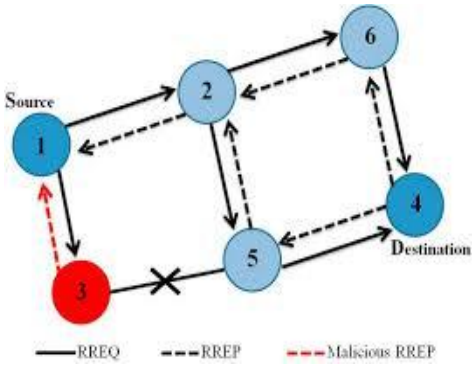

Fig 2: Black hole Attack

Wormhole Attack

A wormhole attack is one of the most sophisticated and severe attacks in WMNs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality.

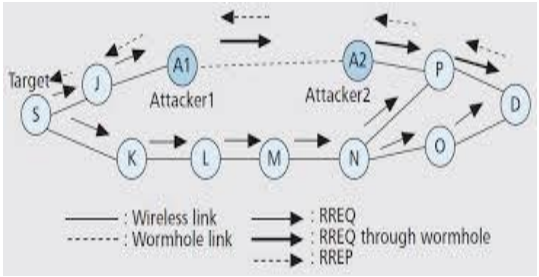

Fig 3: Warmhole attack

In the figure 3, it is assumed that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors J and K forward the RREQ as usual.

However, node A1, which received the RREQ forwarded by node J, tunnels the RREQ to its partner A2. Then, node A2 rebroadcasts this RREQ to its neighbor P. Then RREQ will reach node D. So node D will choose route D-P-J-S to unicast an RREP source node S. As a result, S will select route S-JP- D that indeed passed through A1 and A2 to send its data.

3. Brief Literature Survey

A WMN is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, WMN attracts different real world application areas where the networks topology changes very quickly [7].

However, in [8, 9] many researchers are trying to remove main weaknesses of WMN such as limited bandwidth, battery power, computational power, and security. Although a lot of work under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wired networks cannot be applied directly to WMN, which makes a WMN much more vulnerable to security attacks.

Some solutions in [8, 9, 10] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. Many researchers have developed lots of routing protocols in WMN. The on-demand routing is that set up a route to a target node when ever required in place of static route path. Almost every on-demand routing protocols reestablish a fresh route subsequent to a route break.

Dahill *et al*. Proposed ARAN [11], it assumes managed-open environment, where there is a possibility for predeployment of infrastructure. It is prone to reply attacks using error messages unless the nodes have time synchronization.

Papadimitratos and Haas [12] proposed a protocol SRP that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected and any malicious node can just forge error messages with other nodes as source.

ARIADNE [13], is based on DSR [14] and TESLA [15]. It prevents attackers/compromised nodes from disrupting uncompromised routes comprising of benign nodes. It uses highly efficient symmetric key cryptography. It does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. It is vulnerable to active-1-1 attacker that lies along the discovered route, who does not forward packets and does not generate ERROR if it encounters a broken link. It also requires clock synchronization, which is considered to be an unrealistic requirement for wireless moving networks.

Perlman proposed a link state routing protocol [16] that achieves Byzantine Robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption.

Zhou and Haas [17] primarily discussed key management. They devote a section to secure routing, but essentially conclude 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.

Some work has been done to secure wireless moving networks by using misbehaviour detection schemes [18]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second has no real means to guarantee the integrity and authentication of the routing messages. Looking at the work that has been done in this area previously, it seems that the security needs for wireless moving networks has not been yet satisfied. Most of the work done around using Hashing techniques is around authenticating messages and route table entries.

Bayya *et al*. [19] demonstrate the use of hashing as part of password based authenticated key exchange. The problems in this protocol are the need of a strong shared secret and the need to constantly change the shared secret which in turn may prove to be computationally expensive.

K. Lakshmi *et al*. analyzed and improved the security of one of the popular routing protocol. This work focused specifically, is on ensuring the security against the Black hole Attack. The proposed solution is that capable of detecting and removing black hole nodes in the WMN at the initial stage itself without any delay [20].

S.Taneja [21], proposes a new protocol SSRP (Stable and Secured Routing Protocol). Due to unbalanced node usage, some of the battery powered nodes drain out faster than others. This leads to route re-discovery causing larger average end to end delay and more control overhead. So scheme will be proposed to speed up the process.

4. Security Solutions to Wireless Moving Networks

In AODV protocol, it is assumed that the malicious node has exceptionally large sequence number. Whenever a malicious node joins the network, the packets start dropping and link path breakage happens which in turn loss of data and decrease transfer rate. The proposed scheme will be based on modifications of existing AODV. Two parameters will be considered, one for availability and other for security. In Wireless Moving Network (WMN) it is a performance. Therefore, the scheme will be proposed to make to increase network performance and data transfer reliable. Wireless Moving Network (WMN) is ideally to be used in emergency situations like natural disasters, military conflicts, emergency medical situations etc. Therefore, this research will focus on proposing scheme for providing security to network in unpredictable situations. A protocol will be developed which improves existing on-demand routing protocols by using paper [21] as base. An effort will be made to develop a cryptographic algorithm or to implement new strategy to existing algorithm. The scheme proposed stresses upon applying hashing techniques not only in prevention stage in the form of message and routing information authentication, but also in different stages of securing wireless moving networks.

5. Conclusion

In this paper, it has been analyzed and tried to inspect the security issues in the wireless moving networks, which may be a main disturbance to the operation of it. The evaluation we have presented between the routing protocols indicates that the design of a secure wireless moving routing protocol constitutes a challenging research problem against the existing security solutions. Finally, we consider that more work is still required to justify the exact definition for secure routing which will allow researchers to formally prove whether a proposed protocol satisfies all the security issues concerning wireless

networks. So an effort will be made to develop a cryptographic algorithm or to implement new strategy to existing algorithm. The scheme proposed stresses upon applying hashing techniques not only in prevention stage in the form of message and routing information authentication, but also in different stages of securing wireless moving networks.

6. References

1. Akbani R, Korkmaz T, GVS Raju, HEAP: A packet authentication scheme for mobile wireless networks, Wireless Networks 2008; 6(7):1134-1150.
2. Perrig A, Canetti R, Song D, Tygar D. Efficient and secure source authentication for multicast, In Network and Distributed System Security Symposium (NDSS'01), 2001.
3. T Karygiannis, Owens L. Wireless Network Security, NIST Special Publication 2002, 800-48.
4. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall New Jersey, 2003
5. Yonguang Zhang, Wenke Lee. Intrusion detection in wireless ad-hoc networks, In 6th International Conference on Mobile Computing and Networking (MOBICOM'00), 2000, 275-283.
6. Kush A, Hwang C, Gupta P. Secured Routing Scheme for Adhoc Networks. International Journal of Computer Theory and Engineering (IJCTE). 2009; 3:1793-1799
7. Corson S, Macker J. Mobile Wireless Networking: Routing Protocol Performance Issues and Evaluation Considerations, RFC 2501, 1999.
8. Karakehayov Z. Using REWARD to Detect Team BlackHole Attacks in Wireless Sensor Networks, Wksp. Real-World Wireless Sensor Networks, 2005, 20-21.
9. Kurosawa S. Detecting Blackhole Attack on AODV Based Mobile Wireless Networks by Dynamic Learning Method, Proc. Int'l. J Network Sec. 2006.
10. Zapata MG, Asokan N. Securing Ad-Hoc Routing Protocols, Proc. ACM Wksp. Wireless Sec., 2002, 1-10.
11. Dahill B, Levine BN, Royer E, Shields C. A secure routing protocol for adhoc networks‖, Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, 2001.
12. Papadimitratos P, Haas ZJ. Secure Routing for Wireless moving Networks‖, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002.
13. Adrian Perrig, Johnson DB, Yih-Chun Hu ―ARIADNE: A Secure On-demand Routing Protocol for Adhoc Networks‖, ACM, Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), 2002.
14. Johnson DB, Maltz DA, Hu YC. The Dynamic Source Routing Protocol for Wireless moving Networks‖, Internet Draft, MANET working group, 2003.
15. Perrig R, Canetti Song D, Tygar D. Efficient and Secure Source Authentication for Multicast‖, In Network and Distributed System Security Symposium (NDSS'01), 2001.
16. Perlman R Fault-tolerant Broadcast of Routing Information‖, Computer Networks, 7, 395-405.
17. Zhou L, Haas ZJ. Securing Adhoc Networks‖, IEEE Network Magazine 1999; 13(6):24-30.
18. Marti S, Giuli TJ, Lai K, Baker M. Mitigating Routing Misbehaviour in Wireless moving Networks‖, Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, 2000, 255-265.
19. Bayya Arun. Security in Ad-hoc Networks‖, Computer Science Department, University of Kentucky.
20. Lakshmi K, Manju Priya S, Jeevarathinam A, Rama K, Thilagam K. Modified AODV Protocol against Blackhole Attacks in WMN", International Journal of Engineering and Technology 2008-2010; 2(6):444-449,.
21. Sunil Taneja, Kush A. Stable and Secured Routing Strategy for MANET with SSRP, Global Journal of Computer Science and Technology. 2012; 12(4):1.0.