Research Article **ISSN: 2395 – 5597**

International Journal of Engineering and Robot Technology

Journal home page: www.ijerobot.com

AN INNOVATIVE STUDY OF RDBWS ATTACKS FROM ROUTING PROTOCOL IN MOBILE ADHOC NETWORKS

D. Rajesh*[1] and D. Ramesh[2]

[*1]Department of Computer Science Engineering, Universal College of Engineering and Technology, Tamilnadu, India.

ABSTRACT

Privacy protection of mobile Adhoc Network is more demanding than that of wired Networks. This is due to open nature and mobility of wireless media that required strong privacy protection. RDBWS is efficient for removal of active and passive attacks in MANET. A number of schemes have been proposed to protect privacy in MANET. However none of the protocols avoids all these attacks in a single protocol. In this paper we design a RDBWS protocol with provable secure Routing for unlikability and unobservability for all types of packets. It uses encryption and decryption by means of public encryption scheme. It uses encryption and decryption by means of publickey encryption scheme.

KEY WORDS

MANET-Mobile Adhoc Network and RDBWS-Reply Denial of service Blackhole Warmhole Sybil.

Author of correspondence:

D. Rajesh,

Department of Computer Science Engineering,

Universal College of Engineering and Technology,

Tamilnadu, India.

Email: rajeshd936@gmail.com

INTRODUCTION[1]

In our daily life, several applications require data delivery to destination nodes where the use of routing is an ideal approach to manage the networks. Privacy protection of mobile Adhoc network (MANET) is more demanding than wired networks due to mobility of nodes and open nature of wireless media. In wired networks, one has to access information through wired cables to attackers. The attacker only needs an appropriate transceiver to receive wireless signals without being detected. In wired networks device like desktops is always static and does not move from one place to another. So in wired networks there is no need to protect users. Due to mobility of wireless nodes the sensitive information are kept as secret from the adversaries in wireless media. Otherwise the third parties can harm the information and also damage the information. Privacy protection for Adhoc networks is a risky task due to the minimum band width and high power consumption in wireless devices.

Privacy protection in routing of MANET has a lot of research. There are so many researchers who introduced various routing schemes in MANET. However, existing routing protocol mainly considers anonymity and unlink ability in MANET, most of them uses publickey cryptography to achieve their goals. Existing scheme fails to protect all information from the third party. Until there is no solution to achieve various attacks in MANET and also unlinks ability and unobservability.

Another drawback of existing system is one public key cryptography which has high computation overload that can be reduced by using key exchange scheme[1].

In this paper deals with new proposal for an efficient privacy preserving routing protocol RDBWS that achieves security and content unobservability by employing key exchange scheme. We emphasize that our scheme is to protect all types of packets and it is independent solutions on unobservability.

RELATED WORK

The goal of routing protocols in MANET is to provide minimum path between source to destination with security, minimum overhead and minimum bandwidth. To establish a data transmission between two nodes typically multiple hops are required due to the limited transmission range. Routing protocols can be categorized into proactive, reactive and hybrid protocols, depending on the routing topology[2]. Proactive routing protocols are typically table-driven. Reactive routing protocols do not regularly update the routing information. It moves the nodes when necessary. Hybrid protocols use both proactive and reactive routing protocols.

The protocols in MANET should have the following features.

1. The protocol should provide A-cyclic routing[3].
2. The protocol should change according to the topology.
3. The protocol should have more than one route from source to destination.
4. The protocol should provide high security when packet transmitted.
5. The protocol should have minimum overhead when topology change occurs.

SECURITY NEEDS FOR MANET

MANET continues to grow, so does the need for effective security mechanisms. Because MANET may interact with sensitive data and operate in hostile un attended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing, constrains, security in sensor networks poses different challenges than traditional network security[2].

Data Confidentiality

Data Confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In MANET confidentiality relates to keep the confidentiality of some confidentiality information, we require keeping them secret from all entities that do not have privilege to access them.

Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean data is safe. The adversary can change the data so as to send the network into dis array. For example, a malicious node may add some fragments or manipulate the data with in a packet this new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of malicious node due to the harsh communication environment. The data integrity ensures that only received data has not been altered in transmit.

1. Malicious altering
2. Accidental altering

Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new share keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time .to solve this problem a nonce, or another time related counter, cane added into the packet to ensure data freshness.

Availability

The term availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security standard is challenged mainly during the denial-of service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes do some of the network services unavailable, such as the routing protocol or the key management service.

Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision making process originates from the correct source on the other hand, when constructing the server network, authentication is necessary for many administrative tasks. From the above we can see that message authentication is important for many applications in Adhoc networks. Informally, data authentication allows a receiver to identify that the data really is sent by the claimed sender[4]. In the case of two party communications, data authentication can be achieved through a purely symmetric mechanism the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

PROPOSED WORK

In proposed work the Average Node Speed and Packet delivery latency is implemented using NS2 is shown in Figure No.1 and Figure No.2.

Replay attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed .This is carried out either by the originator or by an adversary who intercepts the data and retransmission it.

Replay attack one generally prevented using some form of freshness mechanism. A typical example is the use of sequence numbers, also known as logical time stamps. However, routing protocols in the network layer generally do not use any freshness mechanisms to protect the replay of data packets. While the IP header includes a sequence number, it is only used to reconstruct a pocket which has been fragmented, so it cannot be related upon to identify unique packets. Sequence numbers are primary used by TCP to maintain the order of packets set via a connection. Although TCP sequence number could be used to ensure freshness, this is not advisable. A related attack arises when there is a TCP connection between two nodes, and a malicious intermediate node reorders packets sent between the two communicating nodes[5].

Denial of Service

A Denial of service attacks (DoS attack) or distributed denial of service attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend service of a host connected to internet[6].

The DoS attacks that target resources can be grouped into three board scenarios. The first attack scenario targets storage and processing resources. This is an attack that mainly targets the memory storage space, or cpu of the service provider. Consider the case where a node continuously sends an executable flooding packet to its neighborhoods and to overload the storage space and delete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes. Neighborhood watch and monitoring can prevent the occurrence of such events by gradually excluding such malicious nodes.

Blackhole Attack

Black hole attack is a kind of Denial of Service (DoS) attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets[4].

During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires[5].

Black hole attack can be done by single malicious node or a group of malicious node, which is known as cooperative black hole attack. Also as we know packet dropping may be done due to various reason like node's malicious behaviour, unavailability of resources, temporary network congestion etc. Sometimes node drops packet only for particular time duration or node drops packets which come from particular source or are meant to be delivered to particular destination. This way they misbehave temporarily. Such nodes or this kind of packet dropping attack is known as Gray hole attack.

Wormhole Attack

For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using a Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at other end[6].

An example is shown in Figure No.3. Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security. The wormhole attack will also affect connectivity-based localization algorithms and protocols based on localization, like geographic routing, will find many inconsistencies resulting in further network disruption.

Sybil attack

Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, and this attack is called Sybil attack. Since Adhoc network depends on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point 'A' to point 'B' .A consequence of this is that attackers have harder time to destroy the integrity of information. However if a single malicious node is able to represent several other nodes the effectiveness of those measure is significant degraded[7].

The attacker may allow all the data or may alter all packets in the same transmission so that the destination nodes cannot detect the change in the packets any more. In trust-based routing environments, representing multiple identities can be used to deliver take recommendations about the trust worthiness of a certain party, home by attracting more traffic to it. In ideal starting point for further attacks amplified if the center of the network, so that if you hear every communication happened inside the network. However in the case of multipath which sends data redundantly not relaying on one path only, the problem of sinkholes can be reduced. Probabilistic protocols which manage the trust worthiness of a network can help detecting sinkholes with in the network.

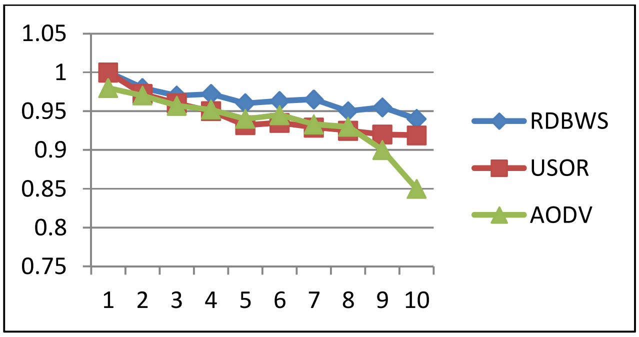

Figure No.1: Average Node Speed

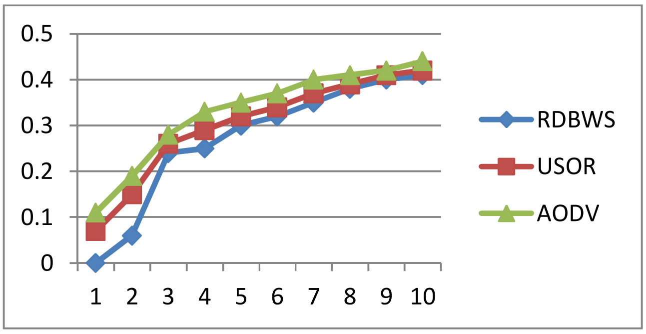

Figure No.2: Packet delivery latency

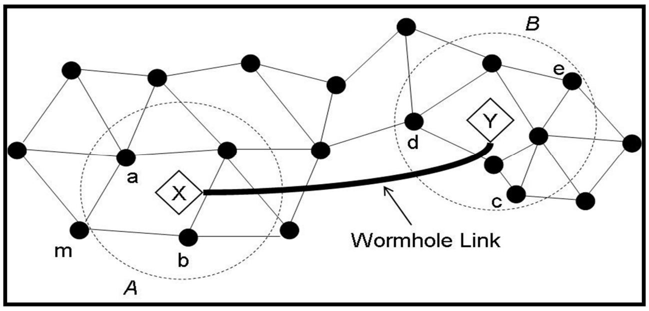

Figure No.3: Wormhole Attack

CONCLUSION

In this project, an RDBWS protocol is proposed based on group signature and ID-based cryptosystem for ad hoc networks. Also this project is proposed to defend against warmhole attacks which cannot be prevented with existing schemes. The design offers strong privacy protection complete unlinkability and content unobservability for ad-hoc networks. The security analysis demonstrates that this protocol not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The protocol is implemented on ns2 and examined the performance of RDBWS, which shows that RDBWS has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I would like to express my gratitude towards my parents and member of Universal College of Engineering and Technology for their kind co-operation and encouragement which help me in completion of this project.

I would like to express my special gratitude and thanks to industry persons for giving me such attention and time.

My thanks and appreciations also go to my colleague in developing the project and people who have willingly helped me out with their abilities.

CONFLICT OF INTEREST

We declare that we have no conflict of interest.

BIBLIOGRAPHY

1. Capkun S, Buttyan L and Hubaux J. "Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, 2(1), 2003, 52-64.
2. Seys S and Preneel B. "ARM: anonymous routing protocol for mobile ad hoc networks," *In Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications*, 2006, 133-137.
3. Zhu B, Wan Z, Bao F, Deng R H and Kankan Halli M. "Anonymous secure routing in mobile ad-hoc networks," *In Proc. 2004 IEEE Conference on Local Computer Networks*, 2004, 102-108.
4. Song L, Korba L and Yee G. "Anon DSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," *In Proc. 2005ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005, 33-42.
5. Boukerche A, El-Khatib K, Xu L and Korba L. "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in *Proc. 2004 IEEE LCN*, 2004, 618-624.
6. Dong Y, Chim T W, Li V O K, Yiu S M and Hui S K. "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," *Ad Hoc Networks*, 7(8), 2009, 1536-1550.
7. Sy D, Chen R and Bao L. "ODAR: on-demand anonymous routing in ad hoc networks," *In 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems*, 2006, 324-329.

Please cite this article in press as: D. Rajesh and D. Ramesh. An Innovative Study of Rdbws Attacks from Routing Protocol in Mobile Adhoc Networks, *International Journal of Engineering and Robot Technology*, 1(1), 2014, 7 - 12.