PRIVACY PROTECTION AGAINST WORMHOLE ATTACKS IN MANET

Mr.B.Satheeshkumar[1], Ms.R.Kalaivani[2]

[1] PG Student, [2]Assistant Professor , Department of Computer Science and Engineering,

PRIST University, Trichy District, India

([1] satheesh.gb@gmail.com)

Abstract

The USOR offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows some keys, the information that the colluding insiders can obtain is largely restricted by USOR. In the padded USOR, all packets including RREQ, RREP packets and other control packets are padded to 128 bytes. Due to the packet padding, performance of the padded USOR is obviously downgraded, but the padded USOR still achieves satisfactory performance: more than 85% delivery success and about 250ms delivery latency. And also it not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. Finally, achieves stronger privacy protection than existing schemes like MASK.

I.INTRODUCTION

1.1 SECURITY MODEL

In this section we first discuss security goals attacks and thus secure routing protocol which is following:
Availability: Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.
Confidentiality: Ensures certain information is never disclosed to unauthorized entities.
Integrity: Message being transmitted is never corrupted.
Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.
Non-repudiation: Ensures that the origin of a message cannot deny having sent the message.
Non-impersonation: No one else can pretend to be another authorized member to learn any useful information.
Attacks using fabrication: Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

1.2 Attack On Ad Hoc Network

There are various types of attacks on ad hoc network which are describing following:
Location Disclosure: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques, or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.
Black Hole: In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network

traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Wormhole: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is *packet leashes.*

Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the off ender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated. Karan Singh, R. S. Yadav, Ranvijay International Journal of Computer Science and Security, Volume (1).

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the *routing table overflow and* the *sleep deprivation torture*.. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Routing Table Poisoning: Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

Rushing Attack: Rushing attack is that results in denial-of-service when used against *all* previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop *Rushing Attack Prevention (RAP)*, a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

Breaking the neighbor relationship: An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session.

Masquerading: During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

Passive Listening and traffic analysis: The intruder could passively gather exposed routing information. Such a attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol

1.3 Routing Security In Ad Hoc Network

The contemporary routing protocols for Ad hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. No single standard protocols capture common security threats and provide guidelines to secure routing. Routers exchange network topology informally in order to establish routes between nodes another potential target for malicious attackers who intend to bring down the network. External attackers injecting erroneous routing info, replaying old routing info or distorting routing info in order to partition a network or overloading a network with retransmissions and inefficient routing.

Internal compromised nodes - more severe detection and correction more difficult Routing info signed by each node won't work since compromised nodes can generate valid signatures using their private keys. Detection of compromised nodes through routing information is also difficult due to dynamic topology of Ad hoc networks. Routing protocols for Ad hoc networks must handle outdated routing information to accommodate dynamic changing topology. False routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there are sufficient numbers of valid nodes, the routing protocol should be able to bypass the compromised nodes, this however needs the existence of multiple, possibly disjoint routes between nodes. Routing protocol should be able to make use of an alternate route if the existing one appears to have faulted Karan Singh, R. S. Yadav, Ranvijay International Journal of Computer Science and Security, Volume (1).

1.4 ROUTING AUTHENTICATION

Routing authentication is one of the important factors in ad hoc networks during route discovery because ad hoc is infrastructure less network. So it is required that a reply coming from a node against a route request must be authentic. That's why authentication protocol is required between the nodes of ad hoc network. In this section we emphasize on the ways by which these protocols can be used.

2. EXISTING SYSTEM

It proposes an efficient privacy-preserving routing protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature. In USOR setup each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme. The unobservable routing protocol is then executed in two phases. First, an anonymous key establishment process is performed to construct secret session keys. Then an unobservable route discovery process is executed to find a route to the destination. Also it provides a thorough analysis of existing anonymous routing schemes and demonstrates their vulnerabilities. The scheme USOR is to protect all parts of a packet's content, and it is independent of solutions on traffic pattern unobservability. And it can be used with appropriate traffic padding schemes to achieve truly communication unobservability.

The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are needed. For the colluding outsiders, privacy information is perfectly protected with USOR. As the attacker is unable to distinguish a meaningful packet from a dummy packet, USOR can provide complete protection for privacy with an appropriate traffic padding scheme. Even if the target node is surrounded by more than one attack node, given the assumption that no node is totally surrounded by compromised nodes, the attacker is unable to perceive anything except some random dummy packets. If appropriate dummy traffic is injected into the network, the colluding outsiders cannot gain any privacy information about the network at all.

3. PROPOSED SYSTEM

3.1 Detecting Wormhole Attacks using Directional Antennas:

Wormhole attacks are the open problem in this existing system. In order to gain the upgraded authentication against the DoS attack, this proposed system "Directional Antenna" provides the efficient restriction against these kinds of malicious attacks.

Directional antenna systems are increasingly being recognized as a powerful way for increasing the capacity and connectivity of ad hoc networks. Transmitting in particular directions results in a higher degree of spatial reuse of the shared medium. The main objective of this system is to find out the neighbors are wormholes are not while keeping its unobservability and unobservability.

Further, directional transmission uses energy more efficiently. This approach to preventing wormhole attacks is for nodes to maintain accurate information about their neighbors (nodes within one hop communication distance). This is simpler than using location since each node need only maintain a set of its neighboring nodes. A message from a non-neighboring node is ignored by the recipient. When sending messages, a node can work in omni or directional mode.

The verified neighbor discovery protocol depends on both neighbor and verifier nodes receiving correct challenge responses from the announcer before either node will accept the announcer as a neighbor. The protocol is secure against wormhole attacks that involve two distant endpoints, since a wormhole can only deceive nodes to accept a particular neighbor if they are in the same relative direction from the wormhole, while the verified neighbor discovery protocol requires that a node receives confirmation from a verifier node in a different direction before accepting a new neighbor. Without acquiring key material, an attacker cannot create a wormhole since it must rely on forwarding messages to legitimate nodes through the wormhole to decrypt the nonce challenges.

Since, this directional antenna provides the session key based connectivity by using the broadcast keys generated by the KGC. Therefore, the properties such as unlinkability and unobservablity are maintained.

4. LITERATURE SURVEY

4.1 Anonymous on Demand routing with untraceable Routes for Mobile Ad-hoc Networks Jiejun Kong, Xiaoyan Ho

A number of anonymous routing scheme have been proposed for ad-hoc networks based on the public key cryptography. ANODR is the first one to provide anonymity and unlinkability for routing in ad hoc networks. Based on onion routing for route discovery, ANODR uses one-time public/private key pairs to anonymity and unlinkability, but in this design the un observable of routing messages is not considered. In ANODR we address two closely related problems:

1. For route anonymity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination.

2. Location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters.

The main drawback of this method is during the route discovery process, each intermediate node creates a one-time public/private key pair to encrypt/decrypt the routing onion, so as to break the link between source and destination.

4.2 Anonymous Secure Routing in Mobile Ad- Hoc Networks Bo Zhu, Zhou Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng

In previous paper works only provide weak location privacy and route anonymity. Therefore we implement the anonymous secure routing protocol that can provide some additional properties on anonymity.

The main objective of this paper is ensuring the security of discovered routes against various active and passive attacks. The anonymous secure routing protocol mainly consists of route request, route response, anonymous data transmission, and route maintenance. Even though it can provide some additional properties the attacker may launch both active attack and passive attack at the same time, and the information obtained from the former can be used to enhance the effectiveness of the later.

Consider one example the adversaries may sniff broadcast data and record the specific that are used to identify the route, and then launch the DOS attack by sending the fake data using the recorded signs.

4.3 Anonymous Routing Protocol for Mobile Ad hoc Networks Stefaan Seys, Bart Preneel and K.U.Leuven

In this paper we present a novel anonymous on demand routing scheme for mobile ad-hoc networks. We identify a number of problems of previous paper and propose an efficient solution that Provides anonymity in a stronger adversary model. The main drawback of ASR and ANODR is efficiency. In this paper the protocol solves the problems related to anonymity and also solving some of the efficiency problems of the previous papers.

So we assume two distinct adversaries.

1. External global passive adversary. The goal of our protocol towards this adversary is to prevent him from learning the destination of these messages, and prevent him from learning which nodes are parts of the path from the source to the destination.

2. Cooperating node inside the network. The goals of our protocol towards this adversary are the node should not be able to determine whether another node in the network is the sender or the destination of a particular message and the second one is the node should not be able to determine whether another node is part of a path between two nodes. Here the communication have been done by based on the following assumption, that is each and every node in the network has a permanent identity that is known by the other nodes in the network that wish to communicate with this node.

4.4 Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks Ronggong Song, Larry Korba, and George Yee

Security, anonymity, and scalability are still important issues for Mobile ad hoc networks. The main drawback of all the previous papers is that can provide only two level of security protection. So we propose a new anonymous dynamic source routing protocol to provide three levels of security protection. The main objectives of this paper are to design a practical trapdoor for anonymous routing. For that we have to use symmetric key trapdoor may be a good choice but it must be designed carefully. The second one is to provide anonymity for all routing and data messages. The last one is scalability. Symmetric key cryptographic operations usually have very good scalability but a public key cryptosystem can provide an efficient way to establish secret session keys for the use of symmetric key cryptosystems.

Based on the above challenges, we have to design the new anonymous dynamic source routing in this section. The new routing consists of three protocols:

- ✓ Security parameter establishment.
- ✓ Anonymous route discovery.
- ✓ Anonymous data transfer.

5. DESIGN OVERVIEW

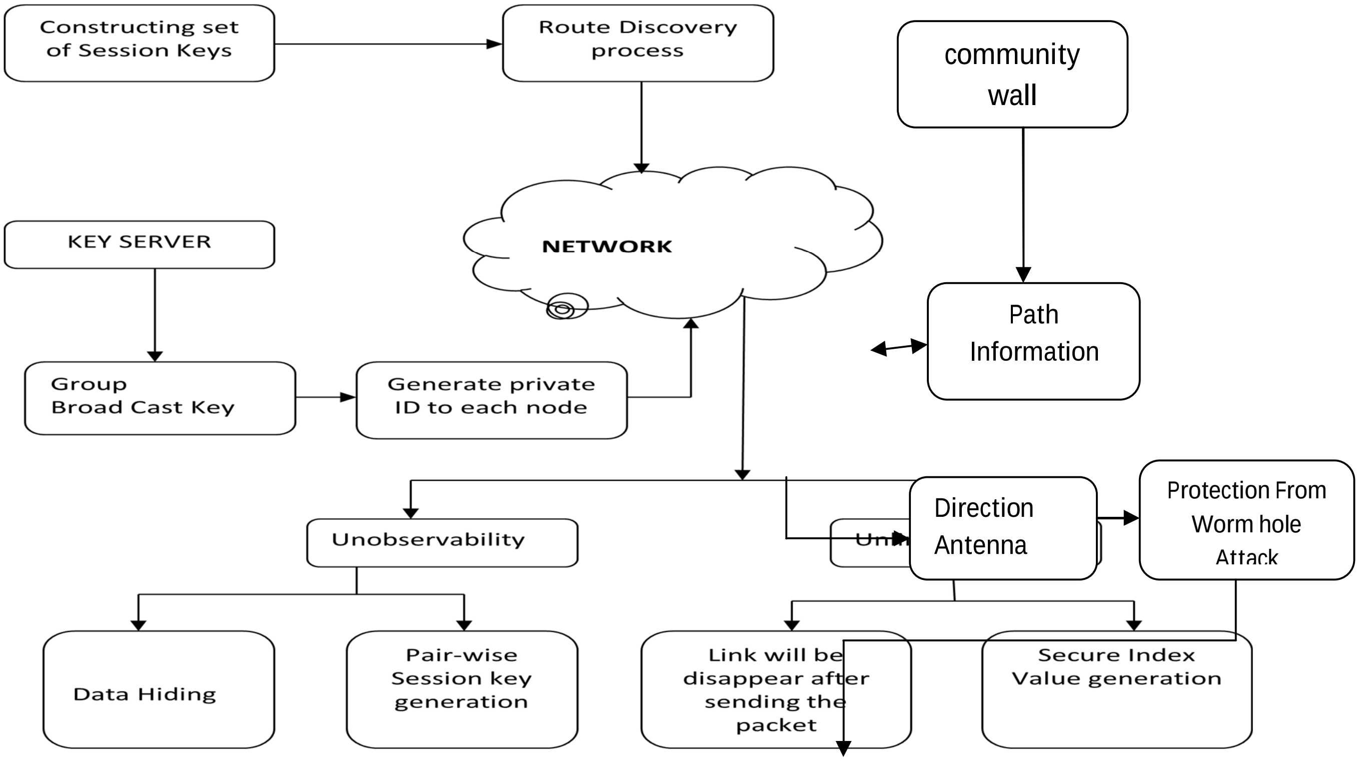
Constructing set of Session Keys
Route Discovery process
community wall
KEY SERVER
NETWORK
Path Information
Group Broad Cast Key
Generate private ID to each node
Unobservability
Uni
Direction Antenna
Protection From Worm hole Attack
Data Hiding
Pair-wise Session key generation
Link will be disappear after sending the packet
Secure Index Value generation

Figure 5-1 : Architecture Of Privacy Protection Against Wormhole Attacks In Manet

6. CONCLUSION

The USOR offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows some keys, the information that the colluding insiders can obtain is largely restricted by USOR. In the padded USOR, all packets including RREQ, RREP packets and other control packets are padded to 128 bytes. Due to the packet padding, performance of the padded USOR is obviously downgraded, but the padded USOR still achieves satisfactory performance: more than 85% delivery success and about 250ms delivery latency. And also it not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. Finally, achieves stronger privacy protection than existing schemes like MASK.

ACKNOWLEDGEMENT

I sincerely thanks to all authors in reference section. All papers in the reference section are very useful for my proposal. Their concepts, algorithms and techniques are very useful for my research.

REFERENCES

[1] Asmidar Abu Bakar, Roslan Ismail, Jamilin Jais, “Forming Trust in Mobile Ad -Hoc Network”, 2009 International Conference on Communications and Mobile Computing (2009)

[2] A Survey on Trust Management for Mobile Ad Hoc Networks Jin-Hee Cho, Member, IEEE, Ananthram Swami, Fellow, IEEE, and Ing-Ray Chen, Member, IEEE

[3] Cook.K.S (editor), Trust in Society, vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York

[4] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based IntrusionDetection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols" in proceedings of IEEE 58th Conference on Vehicular Technology, 2003

[5] Hothefa Sh.Jassim, Salman Yussof, “A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network”, IEEE 9th Malaysia International Conference on Communications (2009)

[6] Hu, Y., "Enabling Secure High-Performance Wireless Ad Hoc Networking,PhD Thesis,Carnegie Mellon University (CMU), (2003)

[7] IIyas M., The Handbook Of Wireless Ad Hoc Network, CRC, (2003)

[8] Kortuem.G., Schneider. J., Preuitt.D, Thompson .T.G.C, F’ickas.S. Segall.Z. “When Peer toPeer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks”, 1st International Conference on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91 (2001)

[9] Mangrulkar.R.S, Dr. Mohammad Atique, “Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network” (2010)

[10] Marc Branchaud, Scott Flinn,"x Trust: A Scalable Trust Management Infrastructure"

[11] Menaka Pushpa.A M.E., “Trust Based Secure Routing in AODV Routing Protocol” (2009)

[12] Sridhar, S., Baskaran, R.: Conviction Scheme for Classifying Misbehaving Nodes in Mobile Ad Hoc Networks in the proceedings of CCSIT 2012 published by Springer (LNICST) 2012

[13] “TAODV: A Trusted AODV Routing protocol for Mobile ad hoc networks” (2009)

[14] Umuhoza.D, J.I. Agbinya., “Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (2007)

[15] Perkins.C E.Royer and S.Das, “Ad hoc on-demand Distance Vector Routing”, RFC-3651