A Literature Survey on Security Challenges in Mobile Ad Hoc Networks

E. Gajendran
Assistant Professor
Dept of Information Technology
CAHCET-Vellore, India

S.Vijayan
Assistant Professor
Dept of Information Technology
CAHCET-Vellore, India

B.Sarvesan
Assistant Professor
Dept of Information Technology
CAHCET-Vellore, India

ABSTRACT
This literature survey summarizes the security challenges and their present solutions in mobile ad hoc network. Basically the ad hoc network is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. Security is an essential requirement in mobile ad hoc network Compared to wired networks; Ad hoc networks are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Especially attacks on mobile ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. In this research paper, identify the existent security threats on ad hoc faces so far, the security services required to be achieved and the countermeasures for attacks in ad hoc routing protocols. Moreover, in this research paper summarize complete literature survey by collecting information related to various types of attacks and its solution. In this research work finally identified the main issues and new proposed solution to overcome them. Further focus on the finding challenges and related works from which to provide highly secure protocol for MANETs.

Keywords
Ad hoc network (AHN), Security attacks, Anonymity Routing algorithms.

1. INTRODUCTION
Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support moveably and organize themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly difficult for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when design a wireless network system. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET).

The MANET require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields, military applications, and other emergency and disaster situations[7].Attacks on ad hoc network can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. For example, traffic analysis is one of the most serious security attacks in MANET [8] here an attacker can identify the communicating parties and their positions by tracing and analyzing the network traffic patterns. This may lead to severe threats in security-sensitive applications. For instance, in a battle field the enemy can physically destroy the important mobile nodes if they can identify and locate such nodes by traffic analysis. In order to thwart such attacks, anonymous communication protocols are developed.

Anonymity is needed in ad hoc network which can improve security by making it difficult for adversaries to trace their potential victims and to conduct target-specific attacks. Achieving node privacy is challenging in ad hoc networks, where routing schemes rely on the cooperation and information exchange among the nodes. In routing algorithm such as AODV [1], [2], DSR [2], and DSDV [2], a node has to disclose its identity (ID) in the network for building a route. Node activities, such as sending or receiving data, are highly traceable and, consequently, nodes are vulnerable to attacks and disruptions. In the reference [17] proposing communication anonymity to thwart the nodes information against opponents. Only the position of the destination node is exposed instead of node identity in the network for route discovery with the limited routing information [17]. In this survey paper finds that the route failure was happened during searching position of the nodes and lack of privacy for the routing.

Secure routing is an important aspect of the ad hoc networks. The routing protocols are like Ad Hoc on Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Topology Dissemi- nation Based on Reverse-Path Forwarding (TBRPF), and Dynamic Source Routing (DSR). Another routing protocol, Dynamic MANET On-Demand (DYMO), is currently in draft state. However, none of these protocols specifies any security measures, effectively assuming that there are no malicious nodes participating in routing operations [1], [2]. In this paper proposing S-AODV in this sense adds security to AODV protocol, based on public key cryptography. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed to guarantee their integrity and authenticity. Therefore, a node that generates a routing message signs it with its private key, and the nodes that receive this message verify the signature using the sender's public key. The hop count cannot be signed by the sender, because it must be incremented at every hop. Therefore, to protect it (i.e., not allow malicious intermediate nodes to decrement it), a mechanism based on hash chains is used. Some times which gets worse when the double signature

mechanism is used, because this may require the generation or verification of two signatures for a single message.

2. SECURITY MODEL

All material in this section are first discuss security goals attacks, anonymous routing and secure routing protocols which are following,

2.1 Security goals for Ad Hoc

The ultimate goals of the security solutions for MANETs[8],[9] is to provide security services, such as authentication, confidentiality, integrity, authentication, non repudiation, anonymity, secure routing and availability to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in MANETs. The common security services are described below

Availability: It 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: It ensures certain information is never disclosed to unauthorized entities.

Integrity: The message being transmitted is never corrupted.

Authentication: It 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: It ensures that the origin of a message cannot deny having sent the message.

Non-impersonation: Which mean no one else can pretend to be another authorized member to learn any useful information.

Attacks using fabrication: which mean that the Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

2.2 Attacks on Ad Hoc Network

There are various types of attacks on ad hoc network which are describing following:

Location Disclosure: It is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [17], 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 it is known as location disclosure.

Black Hole: In a black hole attack a malicious node can inject or insert false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [8]. 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 which types of attack is black hole attack.

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 attacks here, since it involves the cooperation between two malicious nodes that participate in the network [9]. 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 type of attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [1]. Routing table overflow attack the malicious node floods the network with bogus or fake 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 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. So this is known as blackmail attack.

Denial of Service: The most powerful attack in AHN is Denial of service attacks which aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [2]. 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 [1]. 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 [1]. For example, DSR, AODV, and secure protocols based on them, such as 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, an outside intruder could masquerade a 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: In this attack the intruder could passively gather exposed routing information. Such an 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 [12].

Security should be taken into account at the early stage of design of basic networking mechanisms. In this study, first identify the security attacks in each layer and corresponding countermeasures. The following tables summarize the potential security attacks and the actions that can be taken to prevent the attacks.

Table 1 summarizes the attacks and Table 2 represents the solutions in each layer in MANET [1].

Table 1. Security Attacks on each layer in MANET

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding, Traffic analysis, monitoring, disruption MAC (802.11), WEP, Weakness Jamming, interceptions, eavesdropping
Network layer	Wormhole, black hole, Byzantine, flooding, resource consumption, location disclosure attacks.
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

Table 2. Security Solutions for MANET

Layer	Security Issues	Solutions
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses	Adequate security solution Firewalls, IDS etc.
Transport layer	Authentication and securing end-to-end or point-to-point communication through data encryption	Adequate security solution use of public cryptography (SSL, TLS, SET, PCT) etc.
Network layer	Protecting the ad hoc routing and forwarding protocols	No effective mechanism for Source authentication and message integrity mechanisms to prevent routing message modification, but now using some Securing routing protocols (e.g. IPSec, ESP, SAR, ARAN) to overcome black hole, impersonation attacks, packet leashes, SECTOR Mechanism for wormhole attack etc. final solution is inadequate secure routing for ad hoc network
Data link layer	Protecting the wireless MAC protocol and providing link layer security support	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc. finally anonymity is inadequate for ad hoc network.
Physical layer	Preventing signal jamming denial-of-service attacks	Using Spread spectrum mechanisms e.g. FHSS, DSSS etc.

3. ANONYMITY AND SECURE ROUTING ON AD HOC NETWORK

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which they should try to protect the privacy of the nodes from arbitrary disclosure to any other entities [12], [17].

Neither the mobile node nor its system software should default expose any information that allows any conclusion on the owner or current user of the node. In case device or network identifiers are used (eg.MAC address, Internet protocols [IP] address) no linking should be possible between the respective identifier and the rover's identity for the communication partner or any outside attacker.

The main goals of the security routing protocols is consider for attacks on routing can be internally as well as externally, and this means that there is a need to come up with schemes to safeguard the routing process. In this paper survey about the problems in traditional and existing system of internal and external attacks on ad hoc network [16].

3.1 Problem statements

3.1.1 Problems in traditional basic routing algorithms

How to achieve communication privacy, i.e., to prevent the Identities of communication ends from being exposed in mobile ad hoc networks? In anonymity papers [17] which are dealing with privacy for ad hoc nodes. Despite of routing algorithms such as AODV [1], DSR [1], and DSDV [2], a node has to disclose its identity (ID) in the network for building a route. Node activities, such as sending or receiving data, are highly traceable and, consequently, nodes are vulnerable to attacks and disruptions due to lack of position based routing so it's not scalable for routing. In this traditional on-demand routing protocols are face several drawbacks such as network level flooding are used for route discovery. Limited bandwidth makes broadcast and multicast costly in order to avoid the above problems the researcher found position based routing mechanism for node and routing privacy

3.1.2 Problems in traditional position based routing algorithm:

The number of position based routing algorithms for mobile ad hoc network [1], [10] has been developed. As an inherent part of the position-based approach to routing, different schemes for location updates have been presented [1] such as Most Forward with in Radius (MFWR), Nearest Forward Progress (NFP) and Greedy/GEDIR(Geography distance routing) routing schemes which are traditional position routing method are does not guarantee for Anonymity. The privacy weakness in traditional Position Based Routing like as:

(i) An internal attacker can match a position to a node ID through position services. This calls for a secure position service system.
(ii) Local position exchange among neighboring nodes results in extensive information exposure. In addition, the exchange is normally periodic, which gives an attacker great opportunity to obtain the trajectory of a node

3.1.3 Problems in existing secure routing algorithms

The given table 3 will explain about security features in some of the major routing protocols in Ad hoc networks:

Table 3.Existing security features in major routing algorithms [1], [2], [14], and [16]

Algorithms	**Security positives**	**Security Negatives**
OSPF (open shortest path first)	Flooding and information least dependency; hierarchy routing and information hiding; two authentication methods; a simple password scheme and a cryptographic message digest; a digital sign scheme to protect the OSPF routing protocol	public key cryptography very expensive and will slow performance of router; router can generate false routing information.
S-AODV (secure-Ad hoc on demand distance vector routing)	Public key cryptography used	High overhead; possible route discovery corruption
SMT (secure message transmission)	Guarantees integrity, replay protection, origin authentication , and symmetric key cryptography used	Limited protection against compromised topological information
ODMRP (on-demand multicast routing protocol)	-	No security means
AODV (Ad hoc on demand distance vector routing)	Possibly of the use of IP sec	No security means
AO2P (ad hoc on demand position based private routing protocol)	Communication anonymity and privacy enhancement, hide node ID, receiver contention mechanism was proposed	Internal attacks is possible, delay in route searching due to internal attackers
ARMR (anonymous routing protocol with multiple routes for communication in MANT)	Symmetric key, public key operation and hash function was followed, fake route to divert the passive attackers	Active attack may possible

4. SECURITY SOLUTIONS IN THE AD HOC NETWORKS (AHN) SUMMARY

In this paper the above table 3 has revealed that the various kinds of important aspects of security solutions for mobile ad hoc network. Despite of some major positive solution has been given among security on ad hoc routing. So far, very large amount of security negative aspects are existing in ad hoc network which does not clear the above said challenges properly. In this research paper clearly surveyed the security solutions in the ad hoc networks. First, analyze the main

security criteria for the ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. Then point out various attack types that mainly threaten the ad hoc networks. According to these attack types, summarized several security schemes that can partly solve the security problems on the ad hoc networks in future.

5. CONCLUSION AND FUTURE WORK

From the above study, trying to inspect the security threats in ad hoc networks, which may be a main disturbance to the operation of it. Due to nature of mobility and open media AHN are much more prone to all kind of security risks as covered. As a result, the security needs in the AHN are much higher than those in the traditional Ad hoc networks.

During the survey find out some points that can be further explored in the future, such as to find some effective security solutions and protect the AHN from some kinds of security risks. This survey ultimate aim is try to explore deeper in this research area as well as study more features of AHN and exploit their vulnerability. Moreover, this research future aim should be focused to design a set of formalized criteria to evaluate identification algorithms.

6. REFERENCES

[1] I.Ilyas, Mahammad,"The hand books of Ad hoc Wireless Networks-II series" CRC Press LLC, USA.

[2] C.Sivarammurthy,B.S.Manoj,"Adhoc wireless networks-II edition", Pearson education of India.

[3] Elizabeth M. Royer, Charles E. Perkins," An Implementation Study of the AODV Routing Protocol" IEEE 2000, vol no.7803-6596-8/00.

[4] NedaMoghim, FaramarzHendessi, NaserMovehhedinia, "An improvement on wireless ad hoc network routing based on AODV" IEEE 2002, vol.no.7803-7510-06/02.

[5] Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Do-Won Lee, Cheol-Soo Bang, Geuk Lee," A Safe AODV Security Routing Protocol" -International Conference on Convergence and Hybrid Information Technology 2008, IEEE 2008,vol no. 978-0-7695-3328-5/08.

[6] B.Kannhavong, H.Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, page 86, 2009

[7] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. of IEEE Inforcom, 2002.

[8] ALI GHAFFARI "Vulnerability and Security of Mobile Ad hoc Networks" proceeding of the 6th WSEAS international conference on simulation, modeling and Optimization, Lisbon, Portugal, September 22-24, 2006

[9] Lidong Zhou Zygmunt J. Haas,"Securing Ad Hoc Networks" IEEE network, special issue on network security, November/December, 1999.

[10] Toby Xu, Ying Cai," Location safety protection in ad hoc networks", published by Elsevier B.V.-vol no. 1570-8705.

[11] Dijiang Huang, Mayank Verma," ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks", 2009 Elsevier B.V.-vol.no.1570-8705.

[12] Ying Dong, Tat Wing Chimb, Victor O.K. Li, S.M. Yiu b, C.K. Hui,"ARMR: Anonymous routing protocol with multiple routesfor communications in mobile ad hoc networks" 2009 Elsevier B.V.-vol .no. 1570-8705.

[13] Patrick P. C. Lee, IEEE, Vishal Misra, and Dan Rubenstein, "Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks", IEEE 2007-vol.no. 1063-6692.

[14] Davide Cerri and Alessandro Ghioni," Securing AODV: The A-SAODV Secure Routing Prototype" IEEE Communications Magazine in February 2008-vol.no. 0163-6804/08.

[15] Fei Xing, and Wenye Wang," On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures" -IEEE 2010, vol.no.-1545-5971/10.

[16] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani," A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE 2008, vol.no-1553-877X/08.

[17] Xiaoxin Wu and Bharat Bhargava," AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol", IEEE 2005, vol.no. 1536-1233/05.