ISSN 2319-1236

Security Issues in Manet and Counter-Measures

[1]Anthony Adoghe, [2]Ajayi Olujimi, [3]Dike U. Ike, [4]Onasoga Olukayode
[1,2,3,4] Department of Electrical and Information Engineering,
Covenant University, Ota, Ogun state, Nigeria

ABSTRACT

Mobile Ad-hoc Networks (MANET) are self-configuring networks of mobile nodes connected by wireless links. These nodes are able to move randomly and organize themselves and thus, the network's wireless architecture change rapidly and unpredictably. MANETs are usually utilized in situations of emergency for temporary operations or when there are no resources to set up elaborate networks. Mobile Ad-hoc Networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication network, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks due to the nature of the mobile devices (e.g. low power consumption, low processing load). Most of the ad-hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. Apart from security objectives like authentication, availability, confidentiality, and integrity, the ad-hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. In this paper we attempt to survey security issues faced by the mobile ad-hoc network environment and provide a classification of the various security mechanisms. We also analyzed the respective strengths and vulnerabilities of the existing routing protocols and proposed a broad and comprehensive frame-work that can provide a tangible solution.

Indexing terms/Keywords

Keywords: Ad -hoc networks, Security attacks, Secure routing

.Academic Discipline And Sub-Disciplines

Computer and Network Engineering

SUBJECT CLASSIFICATION

Networking Subject Classification

TYPE (METHOD/APPROACH)

Survey

Council for Innovative Research
Peer Review Research Publishing System
Journal: International Journal Data & Network Security (IJDNS)

Vol.3, No.2
editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has caused a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers.

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Individuals and vehicles can thus be inter-connected in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In themobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node’s to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network

2 OVERVIEW OF MANET

Ad-hoc networks are a new technology of wireless communication for mobile hosts. There is no fixed Infrastructure such as base transceiver stations for mobile switching. Nodes within each other’s radio range are able to communicate directly through wireless links. Nodes which are not within each other’s radio range rely on other nearby nodes to relay messages. The wireless nature of communication and lack of any security infrastructure leads to several network security vulnerabilities. Figure 1 shows a comparison between an’ infrastructure ‘cellular network and a ‘non- infrastructure’ mobile ad hoc network.

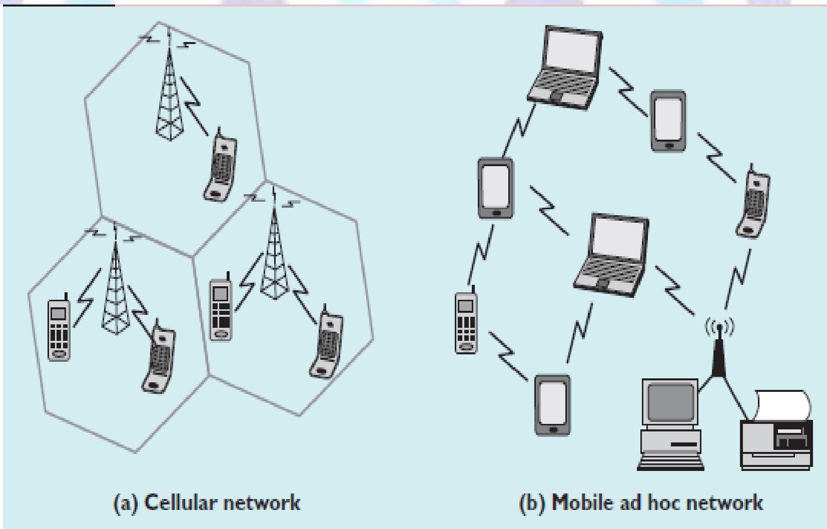

Fig 1: Comparison Between Cellular Network and MANET

In ad-hoc networks information packets are transmitted in a store-and-forward manner from a source to the destination, through intermediate nodes as shown in Figure 2. As the nodes roam, the resulting change in network topology must be relayed to the other nodes so that outdated topology information can be updated or deleted. For example, as N2 in Figure 2 changes its point of attachment from N3 to N4 other nodes part of the network should use this new route to forward packets to N2.

Note that in Figure 2, we assume that it is not possible to have all nodes within range of each other. In case all nodes are close-by within radio range, there are no routing issues to be addressed. In real situations, the power needed to obtain complete connectivity may be, at least, infeasible, not to mention issues such as battery life. Therefore, we are interested in scenarios where only few nodes are within radio range of each other. Figure 2 raises another issue of symmetric (bi-directional) and asymmetric (unidirectional) links. Some of the protocols we discuss consider symmetric links with associative radio range, i.e., if (in Figure 2) N1 is within radio range of N3, then N3 is also within radio range of N1. This is to say that the communication links are symmetric. Although this assumption is not always valid, it is usually made because routing in asymmetric networks is a relatively hard task. In certain cases, it is possible to find routes that could avoid asymmetric links, since it is quite likely that these links imminently fail. Unless stated otherwise, throughout this text we consider symmetric links, with all nodes having identical capabilities and responsibilities.

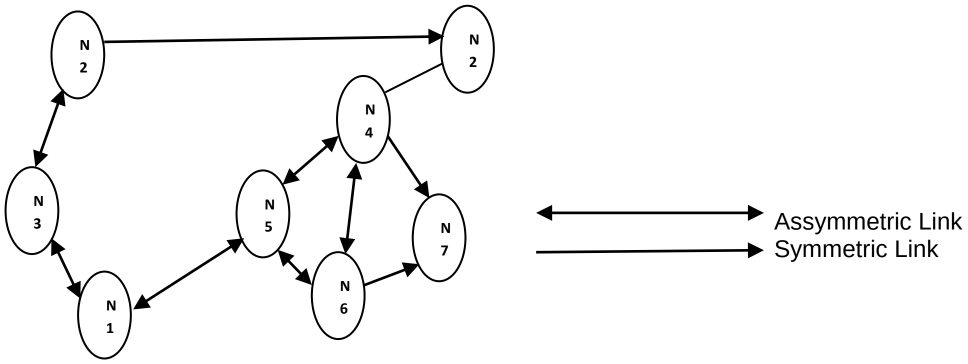

Fig 2: A Mobile Ad-hoc Network

The mobile ad-hoc network has the following typical features [4]: unreliability of wireless links between nodes, constantly changing topology, bandwidth-constrained variable capacity links, power constrained operation, limited physical security, autonomous and infrastructure-less, multi-hop routing, variation in link and node capacities, network scalability. Due to these features, the mobile ad-hoc networks are more prone to network vulnerabilities than the traditional wired networks. Thus, the need to pay more attention to the security issues in mobile ad-hoc networks.

3 MANETS SECURITY ATTACKS AND VULNERABILITY

3.1 WHY MANETS ARE VULNERABLE

Because mobile ad hoc networks are more susceptible to attacks than the traditional wired networks, security is much more difficult to handle in the mobile ad hoc network than in the wired network. In this section, we will discuss the various vulnerabilities that exist in the mobile adhoc networks, which are as follows:

I. Absence Of Secure Boundaries

There is no clear secure boundary in the mobile ad hoc network, as there is in the traditional wired network. Lack of secure boundaries makes the mobile ad hoc network susceptible to various attacks. The attacks mainly include passive eavesdropping, data tampering, active interfering and leakage of secret information, message contamination, message replay and denial of service.

II. Threat From Compromised Nodes Within The Network

Mobile nodes are autonomous units that can join or leave the network at will, it is difficult for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the inherent diversity of different nodes. Also, because of the mobility of the ad hoc network, compromised node can frequently change its attack target and perform malicious behavior to different node in the network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised [5].

III. Lack Of A Central Management Facility

Ad hoc networks do not have a centralized piece of management machinery which lead to some vulnerability problems. Now let us analyze this problem in a more detailed manner.

First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network [6]. Secondly, lack of centralized management machinery will negatively affect the trust management for the nodes in the ad hoc network. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all the network nodes. Thus, it is not practical to perform an a priori classification, and as a result, the usual practice of establishing a line of defense, which distinguishes nodes as trusted and non-trusted, cannot be achieved here in the mobile ad hoc network. Finally, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes. Because there is no centralized decision making infrastructure, the attacker can make use of this vulnerability and perform some attacks that can break the cooperative algorithm.

IV. Unreliable Wireless Links Between Nodes

Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communicating participants.

V. Scalability (Dynamic Topology)

We need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network [4]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale up and down efficiently.

VI. Restricted Power Supply

Some or all of the nodes in a mobile adhoc network may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. The problem that may be caused by the restricted power supply is denial-of-service attack [4]. Since the attacker knows that the target node is battery-restricted, it can either continuously send additional packets to the target, or it can induce the target to be trapped in some kind of time-consuming computation. In this way the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of battery power.

3.2 Attacks On Manets Protocol Stacks

MANET protocol stack attacks include the following:

I. Physical Layer Attacks

a. Eavesdropping- Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency.

b. Jamming- Powerful transmitter with random noise and pulse.

c. Impersonating- Fake messages can be injected into network.

II. Link Layer Attacks

a. Disruption on MAC- A selfish or malicious node could interrupt either contention-based or reservation-based MAC protocols.

III. Network Layer Attacks

a. Wormhole attack- An attacker records packets at one location in the network and tunnels them to another location [9].

b. Black hole attack- First the node exploits the mobile ad hoc routing protocol, such as AODV [12], to advertise itself as having a valid route to a destination node. Second, the attacker consumes the intercepted packets without any forwarding.

c. Routing messages flooding attack- Examples are hello flooding, RREQ flooding, Ack flooding,

d. Resource consumption attack- An attacker can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

e. Location disclosure attack- It gathers the node location information, such as a route map, and then plans further attack scenarios.

IV. Transport Layer Attacks

a. SYN flooding attack- The attacker creates a large number of half opened TCP connections with a victim node, but never completes the handshake to fully open the connection. During the attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets.

b. Session hijacking- The attacker spoofs the victim’s IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

V. Application Layer Attacks

a. Repudiation attack

b. Data corruption- The application layer contains user data, and it normally supports many protocols such as HTTP, SMTP, and FTP. Malicious code, which includes viruses and worms, is applicable across operating systems and applications.

VI. Multi-Layer Attacks

a. Denial of Service (DOS)- Another type of packet forwarding attack is the denial of service (DOS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the mobile ad hoc network.

b. Impersonation attacks- A malicious node can precede an attack by altering its MAC or IP address.

c. Man-in-the-middle attacks- An attacker sits between the sender and the receiver and sniffs any information being sent between two ends.

4 COUNTER-MEASURES TO THE SECURITY CHALLENGES

So far we have discussed the various vulnerabilities in the Mobile Ad-hoc Network. Our aim is not just to point out these vulnerabilities but to also discuss working solutions to the security attacks caused by these vulnerabilities in this network. In this section, we look into some security schemes that can be useful to protect the mobile ad hoc network from malicious attackers.

4.1 Security Attributes

Security level of mobile ad-hoc networks can be analyzed by using the following indices:

I. 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 [4]. This attribute is affected by Denial of Service (DOS).

II. Integrity- Integrity guarantees the identity of the message when they are transmitted. Integrity can be compromised mainly in two ways [7]; Malicious altering and Accidental altering. A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

III. Confidentiality- This means that certain information is only accessible to those who have been authorized to access it.

IV. Authenticity- Authenticity is essentially assurance that participants in the communication network are genuine and not impostors [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity.

V. Authorization- Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified by the certificate authority.

VI. Anonymity- Anonymity means that all the information that can be used to identify the owner or the current user of the node should, by 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 we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

4.2 Approaches to Ensuring Network Security

There are basically two approaches to securing a mobile ad-hoc network: The proactive approach attempts to thwart security threats in the first place, typically through various cryptographic techniques. On the other hand, the reactive approach seeks to detect threats a posteriori and react accordingly. Each approach has its own merits and is suitable for addressing different issues in the entire domain. For example, most secure routing protocols adopt the proactive approach in order to secure routing messages exchanged between mobile nodes, while the reactive approach is widely used to protect packet forwarding operations [8].

4.2.1 *Defense Method Against Wormhole Attacks*

Wormhole attack is a threatening attack against routing protocol of the mobile ad-hoc networks [9]. In the wormhole attack an attacker records bits (or packets) at one point in the network, selectively tunnels them to another location and replays them from there into the network. The replay of the information will make great confusion to the routing issue in mobile ad hoc network because the nodes that get the replayed packets cannot distinguish it from the genuine routing packets. A packet leash is a general mechanism for detecting and, thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. There are two main leashes, which are geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel almost at the speed-of-light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

A geographical leash in conjunction with a signature scheme (a signature providing no repudiation) can be used to catch the attackers that pretend to reside at multiple locations: when a legitimate node overhears the attacker claiming to be in different locations that would only be possible if the attacker could travel at a velocity above the maximum node velocity v, the legitimate node can use the signed locations to convince other legitimate nodes that the attacker is malicious.

Temporal leashes use TIK protocol that implements authentication for broadcast communication in wireless network.TIK stands for TESLA with instant key disclosure, and is an extension of the TESL protocol [10]. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio, or any other range that might be specified. The TIK protocol has been proved to be efficient since it requires just public keys in a network with nodes, and has relatively modest storage, per packet size, and computation overheads.

4.2.2 *Defense Against Blackholes Attacks*

Security-Aware Routing Protocol (SAR) is used. A security metric or trust level added into the RREQ. In the intermediate nodes if trust level is satisfied the node will process the RREQ. The destination generates RREP with the specific security metric. To prevent identity theft stronger access control mechanism is required. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. There indeed have been numerous attempts published in the literature that aim at countering the Black-hole attacks. We survey them in the following. In [11], the authors discuss an approach in which the requesting node waits for the responses including the next hop details, from other neighboring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route-Reply Table) table, whether there is any repeated next-hop-node or not. If any repeated *next-hop-node* is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited. The solution adds a delay and the process of finding repeated next hop is an additional overhead. In [12], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source nodes get this information, it sends a RREQ to the next hop to verify that the target node (i.e the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a Further-Request, it sends a Further-Reply which includes the check result to the source node. Based on information in Further-Reply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request. In [13], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination puts some overhead in one or either intermediate and destination nodes in one or other way.

4.2.3 *Watchdog And Path-Rater*

Watchdog and Path-rater are two main components of a system that tries to improve performance of ad hoc networks in the presence of disruptive nodes, the specific working principles of which are discussed below [14].

Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped match with the observing node’s buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious. Information about malicious nodes is passed to the Path-rater component for inclusion in path rating evaluation.

Path-rater on an individual node works to rate all of the known nodes in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular node’s perspective. Nodes start with a neutral rating that is modified over time based on observed reliable or unreliable behavior during packet routing. Nodes that are observed by watchdog to have misbehaved are given an immediate rating of -100. It should be distinguished that misbehavior is detected as packet mishandling/modification, whereas unreliable behavior is detected as link breaks. It is shown from the experiments that these two components can well reflect the reliability of the nodes based on their packet forwarding performances.

4.2.4 *Localize Self-Healing Approach*

The concept of “self-healing community” is based on the observation that wireless packet forwarding typically relies on more than one immediate neighbor to relay packets. Community-based security explores node redundancy at each forwarding step so that the conventional per-node based forwarding scheme is seamlessly converted to a new per-community based forwarding scheme. Since a self-healing community is functional as long as there is at least one cooperative “good” node in the community, there is no requirement that how many nodes in the community should be available to provide reliable packet forwarding services. There are one configuration and one reconfiguration protocol that can respectively be used to initially set up the self-healing community and fix the community if there is a shape loss due to the mobility or change of topology [15].

4.2.5 *Secure Message Transmission*

A protocol, which, given a topology view of the network determines a set of diverse paths connecting the source and the destination nodes. Then, it introduces limited transmission redundancy across the paths, by dispersing a message into N pieces, so that successful reception of any M-out-of-N pieces allows the reconstruction of the original message at the destination. Each piece, equipped with a cryptographic header that provides integrity and replay protection along with origin authentication and is transmitted over one of the paths. Upon reception of a number of pieces, the destination generates an acknowledgement informing the source of which pieces, and thus routes, were intact. In order to enhance the robustness of the feedback mechanism, the small-sized acknowledgments are maximally dispersed (i.e., successful reception of at least one piece is sufficient) and are protected by the protocol header as well. If less than M pieces were received, the source retransmits the remaining pieces over the intact routes. If too few pieces were acknowledged or too many messages remain outstanding, the protocol adapts its operation, by determining a different path set, re-encoding undelivered messages and re-allocating pieces over the path set. Otherwise, it proceeds with subsequent message transmissions [16].

5 SOLUTIONS TO ATTACKS ON PROTOCOL STACKS

(a) SLSP (Secure Link State Protocol): This protocol [17] provides secure proactive topology discovery .It is responsible for securing the route discovery and distribution of link state information. This protocol is robust against Dos and Byzantine adversaries. But this protocol is still vulnerable to colluding attackers and other attackers.

(b) SEAD (Secure Efficient Adhoc Distance Vector Routing Protocol): It is [18] based on DSDV routing protocol. This protocol is used to guard against Denial of Service by using one way hash functions. It provides limited CPU processing capability. Long lived routing loops can be reduced by using destination sequence numbers. These destination sequence numbers provide replay protection of routing update messages in SEAD.

(c) SAODV(Secure AODV): It is an enhancement over AODV [19] routing protocol that utilizes security feature like integrity and authentication. It uses digital signature to authenticate non mutable field of messages and hash chains to secure hop count information. IPSec provides secure network transmission in MANET for data messages. And digital signature is used when a RREQ is sent between source node to destination node. Primarily sender node signs the message and intermediate node verifies the signature before generating of reverse route to the host. And destination node signs the RREP to its private key.

(d) CONFIDANT (Cooperation of nodes fairness in dynamic adhoc network**):** This algorithm [20] is enhancement of DSR routing and based on selection of selfish and unselfish nodes. Trust and routing calculation process is evaluated by experience, observation and behavior of other nodes, present in the network. It identifies routing misbehavior and maintains the provision of correct forwarding and traffic diversion.

(e) ARAN (Authenticated Routing for Adhoc Networks): ARAN[21] is on demand secure routing protocol an it relies on digital certificates. By using certificate process, it provides authentication, message integrity and non-repudiation. Thus it provides end to end guarantee during message delivery between source and destination. ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. This protocol does not perform well when it is authenticated by selfish node itself and it also leads to wastage of bandwidth.

(f) ARIADNE: It is secure on [22] demand routing protocol and it is based on TESLA concept. TESLA is an efficient authentication scheme that requires loose time synchronization. Firstly it verifies route authenticity and secondly it checks that no node is missing on RREQ message. It is vulnerable to an attacker that happens to be along the discovered route. This routing can authenticate any three schemes: (i) Shared secrets between each pair of nodes (ii) Shared secrets between communicating nodes combined with broadcast authentication or digital signatures. Ariadne needs the security association between the initiator every node including intermediate node and the source node. ARIADNE prevents attackers with uncompromised routes and also prevents many types of Denial-of-Service attacks. But it cannot defend against active 1-1 attack.

(g) ENDAIRA: It is an improved version [23] of ARIADNE and provides solution where ARIADNE fails. It is based on provision on public key system concept. But it cannot defend against man in middle attack. So further there is introduced another secure on demand routing protocol known as ENDIARA Loc.

(h) ENDAIRALoc: This protocol provides solution over man in middle attack as well as wormhole attack. It uses location information of node to resist this attack. It uses pair wise secret keys i.e. symmetric key mechanism rather than public key mechanism. As a result, energy consumption reduces effectively.

(i) PrAODV**:** It is an enhancement of an AODV [24] routing. It uses prediction based routing to reduce route breakages which improves the performance. It maintains two additional parameter in RREP message of AODV such as velocity and location information. These parameters help to calculate predicted link value by which source node can easily predict lifetime of a node.

(j) CORE: Michiardi and Molva has introduced this approach [25]. Suggested algorithm relies on DSR routing. It follows reputation mechanism for monitoring of the cooperativeness of nodes. This mechanism uses the nodes' reputation to forward packets through reliable nodes.

(k) SAR: It is an extension of AODV [26] routing protocol. This protocol considers trust level mechanism to take efficient and secure routing decision. In this a node can find a path through nodes with a particular shared key. It shares symmetric encryption key concept among the nodes. SAR increase overhead due to calculation of encryption and decryption process at each node. It can be implemented using any routing protocol.

(l) BISS (Building Secure Routing out of an Incomplete Set of Security Associations) [27]**:** In this only the destination has security associations established with all nodes on the selected route. The sender will authenticate route nodes directly through security associations and indirectly the nodes which it does not have security associations. The suggested algorithm reduces length ratio. Authentication process can be done by using message authentication codes and digital signatures. It follows RREQ process, same as Ariadne.

(m) TIARA (Techniques for Intrusion resistant, Ad Hoc Routing Algorithms**):** This protocol [28] is used to protect against Resource depletion attack, Flow disruption attack, Route hijacking. This algorithm can be used with any other existing routing protocol.

(n) SRP (Secure Routing Protocol**):** It is an on demand [29] routing protocol. It can discover all possible paths between two nodes. The sole assumption of the protocol is that at the beginning, all the nodes share a group key K and can be trusted. This algorithm is suitable for various applications like military and emergency situations.

(o) SPREAD (Security Protocol for Reliable data delivery): It provides data confidentiality [30] security service in routing protocols. It uses secret sharing scheme between neighboring nodes to strengthen data confidentiality. It overcomes the problem of eavesdropping and colluded attacks.

(p) AODV-SEC: It is an improved version [31] of SAODV and extension of AODV routing protocol. It uses PKI as a trust anchor for node identification using X.509 certificates. X.509 version of AODV-SEC does not scale if the traffic load increases. It may be due to the cryptographic mechanisms.

Each of the above mentioned protocols have their own merits and demerits upon the user requirement a particular protocol may be selected, but no protocol is perfect many researches are going in this field to extend the features of protocols.

6 CONCLUSION

In this paper, we have tried to inspect the security issues in the mobile ad-hoc networks, due to the mobility and open media nature, the mobile ad-hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad-hoc networks are much higher than those in the traditional wired networks. First we briefly introduced the basic characteristics of mobile ad-hoc networks, we then discussed some typical and dangerous vulnerabilities in the mobile ad-hoc networks, most of which are caused by the characteristics of the mobile ad-hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these vulnerabilities has made it necessary to find some effective security solutions to protect mobile ad- hoc networks from all kinds of security risks. Finally, we introduce the current security solutions for mobile ad-hoc networks. We start with the discussion on the security criteria in mobile ad-hoc network, which acts as a guidance to the security-related research works in this area. While researching on the paper, we found some points that could be further explored in the future, such as some aspects of the intrusion detection techniques, we are currently exploring deeper in this research area.

ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards the development of this paper.

REFERENCES

[1] Marco Condi, 2003. Body, Personal and Local Ad hoc Wireless Networks, in Book the Handbook of Ad hoc Wireless Networks (chapter1). CRC press LLC.

[2] M.Weiser, 1991. The Computer for the Twenty-First Century. Scientific American.

[3] M.S.Corson, J.P. Maker and J.H. Cernicione, 1999. Internet-based Mobile Ad hoc Networking,IEEE Internet Computing, pages 63-70.

[4] Amitabh Mishra and Ketan M.Nadkarni, 2003. Security in Wireless Ad hoc Networks, in book The Handbook of Ad hoc Wireless Networks (chapter 30),CRC press LLC.

[5] Wenjia Li and Anupam Joshi, Security Issues in Mobile Ad hoc Networks – A Survey.

[6] Panagotis Papadimitraos and Zygmunt J.Hass, 2003. Securing Mobile Ad hoc Networks,in book The Handbook of Ad hoc Wireless Networks (chapter 31) CRC press LLC.

[7] Data Integrity, from Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Data integrity.

[8] Lidong Zhou, Zygmunt J. Hass, 1999. Securing Ad hoc Networks, IEEE Networks special issue on Network Security.

[9] Y.Hu, A.Perrig and D.Johnson, Packet Leashes, 2003. A Defense against Wormhole Attacks in Wireless Ad hoc Networks, in Proceedings of IEEE INFOCOM'03.

[10] A.Perrig,R.Canetti,J.D. Tygar and D.Song, 2000. Efficient Authentication and Signature of Multicast Streams over Lossy Channels, In Proceeding of the IEEE Symposium on Research in Security and Privacy, pages 56-73.

[11] Latha Tamilselvan. Dr V. Sankarayaran, 2007. Prevention of Blackhole Attack in MANET. The 2nd IEEE international Conference on Wireless Broadband and Ultra Wideband Communications(AUS Wireless 2007) India.

[12] Satoshi Kurosawa,Hidehisa Nakayama,Nei Kato,Abbas Jamalipour,and Yoshiaki Nemoto, 2007. Detecting Blackhole Attack on AODV based Mobile Ad hoc Networks by Dynamic Learning Method. International Journal of Network Security,vol.5.No.3.pages 338-346.

[13] A.Shurman, S.M.Yoo, and S.Park, 2004. Blackhole attack in wireless ad hoc networks.In Proceedings of the ACM 42nd southeast Conference (ACMSE'04), pages96-97.

[14] Jim Parker, Discussion Record for the 1st MANET Reading Group Meeting.http://logos.cs.umbc.edu/wiki/eb/index.php/February-10%2C_2006.

[15] Jiejun Kong,Xiaoyan Hong,Yunjung Yi,JoonSang Park,Jun Liu and Mario Gerlay, 2005. A Secure Ad hoc Routing Approach Using Localised Self-healing Communities, in Proceedings of the 6th ACM International Symposium on Mobile Ad hoc Networking and Computing, pages 254-265,Urbana-Champaign,Illinois.

[16] Panagiotis Papadimitratos, Zygmunt J. Haas, Secure Message Transmission in Mobile Ad hoc Networks.

[17] Panagiotis Papadimitratos, Zygmunt J. Haas, 2003. Secure Link State Routing for Mobile Ad Hoc Networks, Applications and the Internet Workshops Proceedings. 2003 Symposium on 27-31 Jan. 2003 Page(s):379 - 383

[18] Yih-Chun Hu ,David B. Johnson , Adrian Perrig "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks",

[19] Manel Guerrero Zapata, 2006. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draft-guerrero-manetsaodv-06.txt.

[20] Sonja Buchegger, JeanYves Le Boudec,"Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc Networks)", *MOBIHOC'02*

[21] Abdalla Mahmoud Ahmed Sameh Sherif El-Kassas, " Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)"©2005 IEEE

[22] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks." *In* Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (ACM Mobicom*)*, Atlanta, Georgia, September 23 - 28, 2002.

[23] Jing Liu, Fei Fu, Junmo Xiao and Yang Lu. "Secure Routing for Mobile Ad Hoc Networks",

[24] Vinod Namboodiri, Manish Agarwal, Lixin Gao, "A Study on the Feasibility of Mobile Gateways for Vehicular Ad-hoc Networks",*VANET'04,* October 1, 2004, Philadelphia, Pennsylvania, USA.

[25] K. Mandalas, D. Flitzanis, G. F. Marias, P.Georgiadis, " A Survey of Several Cooperation Enforcement Schemes for MANETs"©2005 IEEE

[26] Mohammed Zeshan, Shoab A. Khan, Ahmad Raza Cheema, Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Adhoc Networks"2008 IEEE

[27] Srdjan Capkun, Jean- Pierre Hubaux, "BISS: building secure routing out of an incomplete set of security associations", 2003 IEEE.

[28] Ranga Ramanujan, Atiq Ahamad, Jordan Bonney, Ryan Hagelstrom, Ken Thurber "Techniques For Intrusion-Resistant *Ad* Hoc Routing Algorithms"(C) *2000* IEEE.

[29] Yih-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing" ,May-June 2004IEEE

[30] Wenjing Lou , Wei Liu, Yuguang Fang, " SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks" (C) 2004 IEEE Security and Privacy

[31] Stephan Eichler and Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", ©2006 IEEE