© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Advanced Analysis of KTM and Security Issues in Mobile Ad Hoc Networks

[1]M. Zahir Ahmed, [2]Dr. Syed Nisar Ahmed, [3]Shaik Abdul Muneer, [4]H. Azhar Salam

[1,2,3]Lecturer in Physics, Department of Physics, Osmania College, Kurnool, Andhra Pradesh, India
[4]Lecturer in Electronics, Dept. of Physics, Osmania College, Kurnool, Andhra Pradesh, India

ABSTRACT

An ad hoc Network is a new generation of network offering unrestricted mobility without any underlying infrastructure. In this kind of network, all the nodes share the responsibility of network formation and management. This paper proposes a five-layer security architecture for ad hoc networks, that provides self organized distributed security, and authenticated, security aware routing. This model has been simulated and is found to provide security with negligible overhead Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. The performance evaluation have their place in wireless network research, the current and future applications of the ad hoc networks have forced the research community to look at dependability and security aspects as eavesdropping and jamming. To develop suitable security solutions for such new environments, we must first understand how MANETs can be attacked. This chapter provides a comprehensive survey of attacks against a specific type of target, namely the routing protocols used by MANETs. We introduce the security issues specific to MANETs and present a detailed classification of the attacks/attackers against these complex distributed systems. Then we discuss various proactive and reactive solutions proposed for MANETs. It then addresses the possible solution to protect the security mechanism, which involves availability, integrity, authentication and non repudiation. These securities related issues are well addressed if one can provide methods that are pertinent for authentication, key distribution, and intrusion detection and rerouting in case of Byzantine failure in MANETS. Depending on the application context, a user may desire various security services such as authentication, integrity, non-repudiation, Confidentiality,(KTM) Key and Trust Management and access control.

Keywords: Routing, non-repudiation, Byzantine failure, MANET, Security, Authentication, Integrity, Non-repudiation, Confidentiality, Key and Trust Management(KTM).

I. INTRODUCTION

Ad hoc wireless network is a collection of wireless mobile nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. As shown in fig 1. Ad hoc networks structure use mobile nodes to enable communication outside wireless transmission range. 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[1]. Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. The general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. Without one of these parameters, security will not be complete. Without authentication, an attacker could masquerade a node, thus being able to have unauthorized access to the resources and to sensitive information.

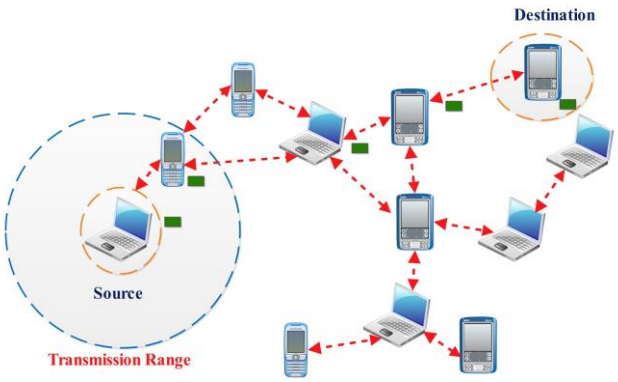

Figure 1 : Manet Structure

In this paper we attempt to analyze various security issues. The provision of security services in MANET is dependent on the characteristics of the supported application and the networked environment, which may vary significantly. The common assumption that MN credentials (e.g., certificates) are bound to IP addresses may need to be revisited, because one can imagine that roaming MNs will joint MANET sub domains and IP addresses will be assigned dynamically (e.g., DHCP) or IPv6 auto configuration or even randomly (e.g., Zero-Configuration A type of ad hoc network with particular requirements is a sensor network, which requires multi-hop communication throughout a network of hundreds or even thousands of MNs, with relatively infrequent topological changes[2]. It is expected that a single organization will undertake the deployment and administration of these networks.

II. Key Management Scheme

Moreover, sensing devices have limited computational capabilities, network transmission rates are relatively low, and communications are mostly data driven. The design of security measures for sensor networks, as demonstrated by the schemes proposed in the many literatures. One of the proposals to secure sensor networks provides a protocol for data authentication, integrity, and freshness and a lightweight implementation of an authenticated broadcast protocol. An approach that has similarities but targets a more general setting proposes a key management scheme for sensor networks[3]. The focus is on resource-constrained large sensor networks, comprising MNs that are assumed tamper-resistant and equipped with a secret group key. Similar to the previous scheme, the use of symmetric key cryptography is proposed as the only feasible, low-cost solution. In mobile ad hoc networks, security depends on several parameters (authentication, Confidentiality, integrity, non-repudiation and availability).

2.1. Multi-Hop Communication:

In ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication: nodes that are within each other's radio range can communicate directly via wireless links, while those that are far apart must rely on intermediate nodes to act as routers to relay messages. Mobile nodes can move, leave and join the network and routes need to be updated frequently due to the dynamic network topology. A variety of new protocols have been developed for finding/updating routes and generally providing communication between end points[4] (but no proposed protocol has been accepted as standard yet). However these new routing protocols, based on cooperation between nodes, are vulnerable to new forms of attacks. Unfortunately, many proposed routing protocols for MANETs do not consider security. Moreover their specific features -the lack of central points, the dynamic topology, the existence of highly-constrained nodes, presents a particular challenge for security.

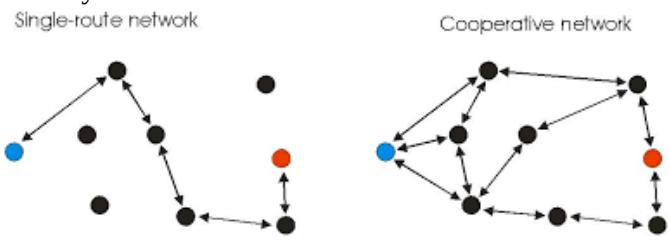

Figure 2 : Multi-hop Communication

2.2. Intelligent Vehicular Ad Hoc Network:

Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Intelligent vehicular ad hoc networks (In VANETs) use WiFi IEEE 802.11p (WAVE standard)and WiMAX IEEE 802.16

for easy and effective communication between vehicles with dynamic mobility[5]. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. In VANET is not foreseen to replace current mobile (cellular phone) communication standards. "Older" designs within the IEEE 802.11 scope may refer just to IEEE 802.11b/g. More recent designs refer to the latest issues of IEEE 802.11p (WAVE, draft status). Due to inherent lag times, only the latter one in the IEEE 802.11 scope is capable of coping with the typical dynamics of vehicle operation. Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. The advantage of WiFi based navigation system function is that it can effectively locate a vehicle which is inside big campuses like universities, airports, and tunnels. In VANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity.

III. Wireless Links of MANETs

Wireless Links: First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access tothe network to carry out these attacks. Furthermore wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes. Dynamic Topology: MANET nodes can leave and join the network, and move independently[6]. As a result the network topology can change frequently. It is hard to differentiate normal behavior of the network from anomaly/malicious behavior in this dynamic environment. For example, a node sending disruptive routing information can be a malicious node, or else simply be using outdated information in good faith. Moreover mobility of nodes means that we cannot assume nodes, especially critical ones (servers, etc.), are secured in locked cabinets as in wired networks. Nodes with inadequate physical protection may often be at risk of being captured and compromised[7]. Cooperativeness: Routing algorithms for MANETs usually assume that nodes are cooperative and non malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. For example, a node can pose as a neighbor to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly.

IV. Related Work

We classify related work to ad hoc network security into the following three categories:

4.1. Basic security infrastructure: MANET is a network without any basic infrastructure; hence there is no trusty relationship like PKI for all the participating nodes in MANETs. The first step to establish a security system is to setup the basic security infrastructure and establish security associations between communicating nodes.

4.2. Secure routing: In the ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks. Unlike fixed networks, routing information in an ad hoc network could become a target for adversaries to bring down the network. There are two types of threats. The first one comes from external attackers. The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. With these ways, the attackers can successfully partition a network or introduce excessive traffic load into the network, thus cause retransmission and ineffective routing[8]. The set of applications for MANETS is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETS need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETS. Factors such as variable wireless link quality, propagation path loss, fading, multi-user interference, power expended, and topological changes, become relevant issues.

Figure 3. Mobile Ad Hoc Network Applications

V. Routing in Ad-Hoc Networks

Mobile Ad-Hoc networks (MANETS) are by definition peer-to-peer, multi-hop networks, without any existing infrastructure. If a network host wishes to communicate with another network host that is outside its radio range, it must use intermediate hosts to route the communications. Therefore routing functionality needs to be incorporated into the mobile hosts[9]. In wired networks routing algorithms are categorized as link state based protocols (e.g. OSPF Open Short Path First) or distance vector based (e.g. RIP Routing Information Protocol). The link state protocols use the Dijkstra algorithm. Link state advertisements are sent to all network routers. The routers accumulate link-state information and the Dijkstra algorithm is used to calculate the shortest path to each node. The distance vector based protocols use the Bellman-Ford algorithm.

5.1. DSDV Protocol

Destination Sequenced Distance Vector routing is a table-driven routing protocol based on the Bellman-Ford algorithm[10]. The modification for ad-hoc networks is that routing loops are avoided. Each network node maintains its own routing table in which all destination nodes in the network and the numbers of routing hops are recorded. Routing information is always available, whether a route is required or not by a source node. Routes are given a sequence number to distinguish stale routes from new ones. Routing table updates are sent periodically throughout the network to maintain consistency. To reduce the amount of network traffic that this produces, table updates are sent as smaller incremental updates during periods of low mobility. During periods of high mobility, full table updates are distributed. As new routes are added to the tables, they include the destination node address and the number of hops. The route with the most recent sequence number (indicating freshness) is always used. If two routes have the same sequence number then the one with the smaller hop count is used.

5.2.AODV Protocol

The Ad Hoc On-Demand Distance Vector (AODV) builds on the DSDV protocol by minimizing the required number of broadcasts by creating routes on a source initiated, on-demand basis. There is no requirement to maintain a complete list of routes[11]. When a source node wants to communicate with a destination node, it broadcasts (multicasts, if IPv6 is being used) a route request (RREQ) packet to its neighbors.

VI. Authentication

Authentication enables a MN to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. III. NON-

6.1. Repudiation

It ensures that the original message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised MNs. Ensures that sending and receiving parties can never deny ever sending or receiving the message.

6.2. Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality.

VII. Key and Trust Management

Key and trust management is a critical supporting element in any security systems. Its basic

operations include establishing key exchange and update, as well as secret connections. Keys are the basic blocks of symmetric and asymmetric cryptographic functions, which in turn furnish authentication, confidentiality, integrity, and non-repudiation security services. The main body of key and trust management in MANETs is concerned with a hybrid of asymmetric and symmetric cryptosystems, where trust is established via credential verification, and shared secrets are exchanged for latter use in efficient symmetric cryptosystems.

Step1

```
time = tsync
clock(time)
P = large prime number
i = 0
neigh = 0
repeat
        n = neighbour id
        table[i] = node_id * n mod P
        i++
until(neighbour ≠ ϕ)
repeat
        i = nonce
        time_stamp = clock()
        inv_i = EXTENDED EUCLID(P,i
        hash_table(time_stamp,inv_i, i)
forever
```

Step 2: Data Transmission

```
a1 = node_id
repeat
        t = latest time stamp present in hash
        ii = hash_table.t.i
        b1 = a1^ii mod P
        enc_data = b1.time_stamp.E(K,data)
forever
```

Step 3: Detection

```
a2 = node_id
repeat
        bb1 = enc_data- > b1
        time_st = enc_data- > time_stamp
        if(hash_table.time_st ∈ hash_table)
                i'= hash_table.time_st.inv_i
                check = (a2^inv_i * b1) mod P
                if(check ∈ table[])
                data transmission routine is
                called and data is forwarded
                else
                        data is discarded
        else
                data is discarded
forever
```

An inherent issue in trust management is the trust graph, where the MNs correspond to the network entities and edges to the verifiable credentials. The security in networking is in many cases dependent on proper key management. Key management consists of various services, of which each is vital for the security of the networking systems.

VIII. Security of Key Management

As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As shown in fig 4. ad hoc networks shows no. of attacks in data transmission and calculation of delay significantly vary from each other in many respects, an environment-specific and efficient key management system is needed. To be able to protect nodes e.g. against eaves dropping by using encryption, the nodes must have made a mutual agreement on a shared secret or exchanged public keys.

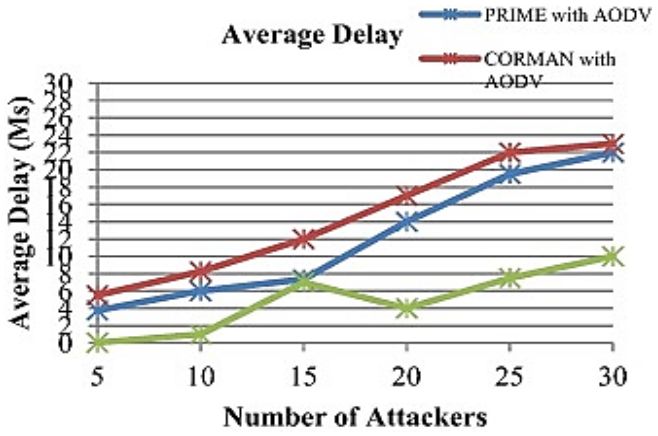

Figure 4. Number of Attacks in MANETS

For very rapidly changing ad hoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumptions about a priori negotiated secrets[11,12]. In less dynamic environments like in the classroom example above, the keys may be mutually agreed proactively or even configured manually (if encryption is even needed).

IX. Conclusion

In this work It is clear that the security aspects related to ad hoc networks form a very complex problem fields, given the dynamic and unpredictable nature of most ad hoc networks. Since proposed routing protocols on MANETs are insecure, we have mainly focused on active routing attacks which are classified into dropping, modification, fabrication, and timing attacks. Attackers have also been discussed and examined under insider and outsider attackers. Insider attacks are examined on our exemplar routing protocol AODV. Conventional security techniques are not directly applicable to MANETs due to their very nature. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. On the other hand, ad hoc networks vary from each other greatly from the viewpoint of the area of application. Some ad hoc networks may not need security solutions other than simple encryption and username-password authentication scheme. In this work we have dealt with security issues in mobile ad hoc networks. We have focused on designing a security architecture in tackling security challenges mobile ad hoc networks are facing[12]. We present a security architecture in a layered view and analyze the reasoning for such a security architecture, and apply the proposed security architecture in military scenarios. In this chapter we summarize secure routing approaches proposed for MANETs. The difficulty of key management on this distributed and cooperative environment is also discussed. Furthermore we have surveyed intrusion detection systems with different detection techniques proposed in the literature. Each approach and technique is presented with attacks they can and cannot detect. To conclude, MANET security is a complex and challenging topic. We expect this security architecture can be used as a framework when designing system security for ad hoc networks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for security mechanisms.

X. REFERENCES

[1]. Buchegger S., Tissieres C., Le Boudec J.-Y.,"A Test-Bed for Misbehaviour Detection in Mobile Ad-Hoc Networks –How Much Can Watchdogs Really Do?", Mobile Computing Systems and Applications (WMCSA '04), pp. 102-111, 2004

[2]. Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003

[3]. Stajano F., Anderson R., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", In Proc. of Int. Workshop on Security Protocols, Springer, 1999 Yi P., Dai Z., Zhang S., Zhong Y., "A New Routing Attack in Mobile Ad Hoc Networks", Int.

[4]. Hattig .M, 2001, Ed., Zero-Conf IP Host Requirements, Draftietfzerofonfreqts- 09.tct, IETF MANET Working Group, August 2001.

[5]. Perrig .A, Szewczyk .R, Wen .V, Culler .D, and Tygar J.D, 2001, "SPINS: security protocols for sensor networks": Proceedings of the 7th Annual

International Conference in Mobile Computing and Networks (MobiCom 2001), Rome, Italy, pp. 189–199.

[6]. Basagni .S, Herrin .K, Rosti .E, and Bruschi .D, 2001, "Secure Pebble nets, in: Proceedings of 2nd MobiHoc", Long Beach CA, October 2001, pp.156–163.

[7]. Boukerche .A, El-Khatib .K, Xu .L,Korba .L, 2004, "Secure ad hoc routing protocol", Fourth International IEEE Workshop on Wireless Local Networks. Tampa, Florida, November 2004. NRC47394.

[8]. Pearlman .M. R, Haas .Z .J, Sholander .P, Tabrizi S. S,"On the impact of lternate path routing for load balancing in mobile ad hoc networks", Mobi HOC, 2000.

[9]. Yenumula B. Reddy, RastkoSelmic. 2011, "Agentbased Trust Calculation in Wireless Sensor Networks", SENSORCOMM 2011: The Fifth International Conference on Sensor Technologies and Applications, IARIA, pp 324-339.

[10]. Wenjia Li, Anupam Joshi And Tim Finin, 2011 "ATM: Automated Trust Management For Mobile Ad-Hoc Networks Using Support Vector Machine", In: 12th IEEE International Conference On Mobile Data Management (MDM), pp. 291–292

[11]. Govindan and P. Mohapatra, 2012 "Trust computations and trust dynamics in mobile adhoc networks: A survey, "IEEE Commun. Surveys & Tutorials, vol. 14, no. 2, pp. 279–298.

[12]. England, P., Shi, Q., Askwith, B., Bouhafs. 2012, " A Survey Of Trust Management In Mobile Ad-Hoc Networks "Proceedings of the 13th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting.

Author Profile

[1]. M. Zaheer Ahmed, Lecturer in Physics and HOD of Dept. of Physics, is doing various research activities. He published articles and research papers in reputed international journals. He had 28 years of teaching experience in Physics and Communications, His qualification is M.Sc., and pursuing PhD. He is interested in Research activities related to wireless communication and network security and Thermodynamics. He has organized many Seminars.

[2]. Dr.Syed Nisar Ahmed, Lecturer in Physics, is doing various research activities. He published articles and research papers in reputed international journals. He had 26 years of teaching experience in Physics and Communications, He is interested in Research activities related to wireless communication and network security and Electro Magnetic Radiation.

[3]. Shaik Abdul Muneer, Lecturer in Physics, is doing various research activities. He published articles and research papers in reputed international journals. He had 22 years of teaching experience in Physics and Communications, He is interested in Research activities related to wireless communication and network security and Electromagnetics.

[4]. H. Azhar Salam, Lecturer in Electronics, is doing various research activities. He published articles and research papers in reputed international journals. He had 28 years of teaching experience in Physics and Communications, He is interested in Research activities related to wireless communication and network security and Optics.