INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 5 (2016) PAGES 1244 - 1249
RECEIVED : 29/09/2016. PUBLISHED : 16/10/2016

A SECURE ARCHITECTURE & EFFICIENT MANAGEMENT IN MOBILE AD HOC NETWORKS

B.Uma[1] , Dr. J.Dhillipan[2] , D. B. Shanmugam[3],
[1]MPhil., Research Scholar, Dept. of Comp.Sci,Dr. MGR. Chockalingam Arts College, Arni.
[2]Asst.Prof.,(S.G) &amp; Head, MCA Department, SRM University, Ramapuram Campus, Chennai,
[3]Asso.Prof., Dept. of Comp.Sci, Dr. MGR.Chockalingam Arts College, Arni.

Abstract:

A layered architecture can provide such advantages as modularity, simplicity, flexibility, and standardization of protocols. Follow this thought, we present here a layered secure architecture for MANETs. In mobile ad hoc networks, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. 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. Fundamental characteristics of a mobile ad hoc network, such as open medium, dynamic topology, dynamic cooperation and constrained capabilities lead to vulnerabilities. Unlike wired network, an ad hoc network does not have a clear line of defense, and every node must be prepared for encounters with an adversary. This thesis 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. We propose a secure and efficient key management (SEKM) framework for mobile ad hoc networks. SEKM builds a public key infrastructure (PKI) by applying a secret sharing scheme and using an underlying multi-cast server groups. We give detailed information on the formation and maintenance of the server groups. In SEKM, each server group creates a view of the certificate authority (CA) and provides certificate update service for all nodes, including the servers themselves. A ticket scheme is introduced for efficient certificate service. In addition, an efficient server group updating scheme is proposed. The performance of SEKM is evaluated through simulation.

Keywords – Dynamic topology, PKI, SKEM, CA.

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without help from a network infrastructure. Each device in a MANET is free to move independently in any direction and will therefore change its link to other devices frequently. Each must forward traffic unrelated to its own use and therefore be a router. The primary challenge in building a (MANET) is equipping each device to continuously maintain the information required to properly route traffic. MANET is infrastructure because in MANET the collection of nodes capable of communicating with each other without help from a network infrastructure. MANETs are a kind of wireless ad-hoc network that usually has a routable network environment on top of a link layer ad-hoc network. They are also a type of mesh network but many mesh networks are not mobile or not wireless. With the increase of portable devices as well as progress in wireless communication, ad hoc networking is

Fig.1. Mobile Ad hoc Network

gaining importance with the increasing number of widespread applications. Applications of MANETs include the battlefield applications in which Military equipment now routinely contains some sort of computer equipment, Commercial sector. Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake, Local level. Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants as Personal Area Network (PAN). Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). With the increasing number of applications to harness the advantages of Ad Hoc Networks, more concerns arise for security issues in MANETs.

2. RELATED WORK

There are five main security services for MANETs: authentication, confidentiality, integrity, non-repudiation , availability. Authentication means that correct identity is known to communicating partner; Confidentiality means certain message information is kept secure from unauthorized party; integrity means message is unaltered during the communication; non- repudiation means the origin of a message cannot deny having sent the message; availability means the normal service provision in face of all kinds of attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered. Once authentication is achieved in MANET, confidentiality is a matter of encrypting the session using whatever key material the Communicating party agree on. Note that these security services may be provided singly or in combination. A mobile ad hoc networks is a special type of wireless network in which a collection of mobile hosts with wireless network interfaces may form a temporary network, without the aid of any fixed infrastructure or centralized administration. In mobile ad hoc networks, nodes within their wireless transmitter ranges can communicate with each other directly (assume that all nodes have the same transmission range), while nodes outside the range have to rely on some other nodes to relay messages. Thus a multi-hop scenario occurs, where the packets sent by the source host are relayed by several intermediate hosts before reaching the destination host. Every node functions as a router. The success of communication highly depends on the other nodes' cooperation. While mobile ad hoc networks can be quickly and inexpensively set up as needed, security is a more critical issue compared to wired or other wireless counterparts.

3. ROUTING APPROACHES HOC NETWORKS

Many of these routing protocols have been designed based on similar sets of assumptions. For instance, most routing protocols assume that all nodes have homogeneous resources and capabilities. This includes the transmission ranges of the nodes. Also, bidirectional links are often assumed. In some instances, protocols have mechanisms for determining whether links are bidirectional. In these cases, the protocols will then eliminate unidirectional links from consideration for routing. The defining characteristics of ad hoc networks include resource-poor devices, limited bandwidth, high error rates, and a continually changing topology. Among the available resources, battery power is typically the most constraining. Hence, the following are typical design goals for ad hoc network routing protocols.

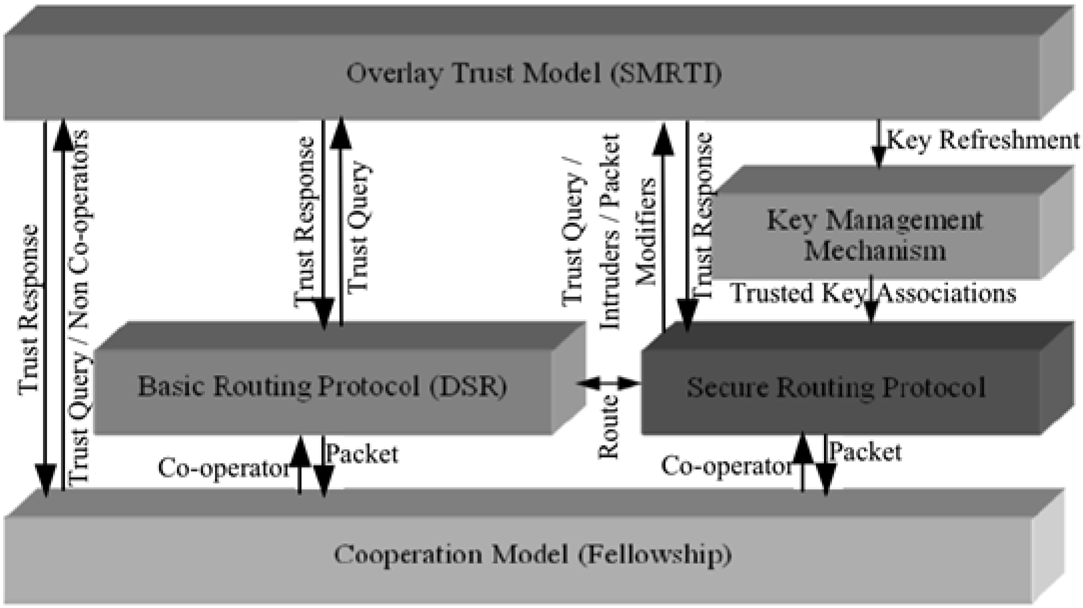

Fig.2. Trust Enhanced Secure Architecture for MANET.

The primary characteristic of proactive approaches is that each node in the network maintains a route to every other node in the network at all times. Route creation and maintenance is accomplished through some combination of periodic and event-triggered routing updates. Periodic updates consist of routing information exchanges between nodes at set time intervals. The updates occur at specific intervals, regardless of the mobility and traffic characteristics of the network. Event-triggered updates, on the other hand, are transmitted whenever some event, such as a link addition or removal, occurs. The mobility rate directly impacts the frequency of event-triggered updates because link changes are more likely to occur as mobility increases. Rather than visualising the Scasec, the SMG and the DSR as separate sub-systems, we can consider them as an amalgamated hybrid sub-system for the purpose of interface integration because of their tight coupling and dependency on each other. Initially, the main integration objective is to facilitate the Scasec to asynchronously report benign and malicious behaviours to the SMRTI's detection component. The Scasec is integrated with the fellowship so that it processes incoming packets after they have been sanitised by the rate-limitation component, and dispatches the packets for transmission once the enforcement component has given the go ahead signal.

4. SIMULATION AND ANALYSIS

Routing protocols for ad hoc networks are challenging to design. Wired network protocols (such as BGP) are not suitable for an environment where node mobility and network topology rapidly change. Such protocols also have high communication overhead because they send periodic routing messages even when the network is not changing.

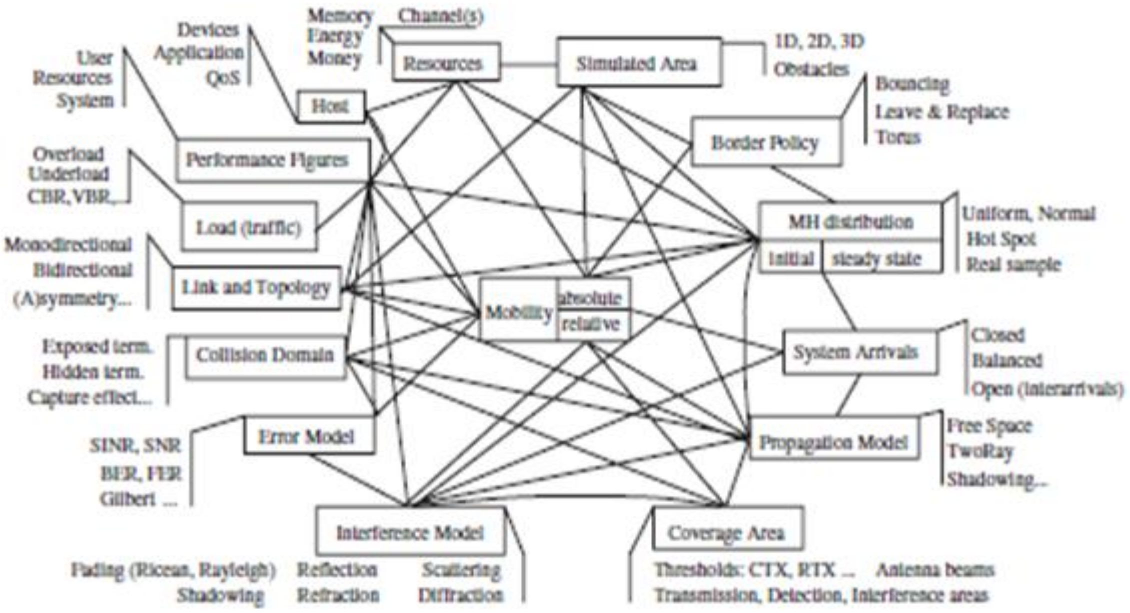

Fig.3.The Modeling Roadmap

So far, researchers in ad hoc networking have studied the routing problem in a non adversarial network setting, assuming a reasonably trusted environment. However, unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks, those functions are carried out by all available nodes. This very difference is at the core of the increased sensitivity to node misbehavior in ad hoc networks, and the current proposed routing protocols are exposed to many different types of attacks. Network layer security module functions Similar to the mac layer, divide into four main functional areas. First, the authentication information encapsulation area. In the routing maintenance control packets encapsulate authentication information for periodic authentication provides relevant packet. Second, trusted level recording area. Different to mac layer, trusted level list record a variety of properties (≥3 kinds) rather than trusted list that record only two properties about yes or no, and it can be extended to a more detailed list of multi-level in order to accommodate the needs of different security environment. There are four trusted levels designed here (Trusted, Medium, Black, Unknown, of course you can design more detailed levels). Third, signature

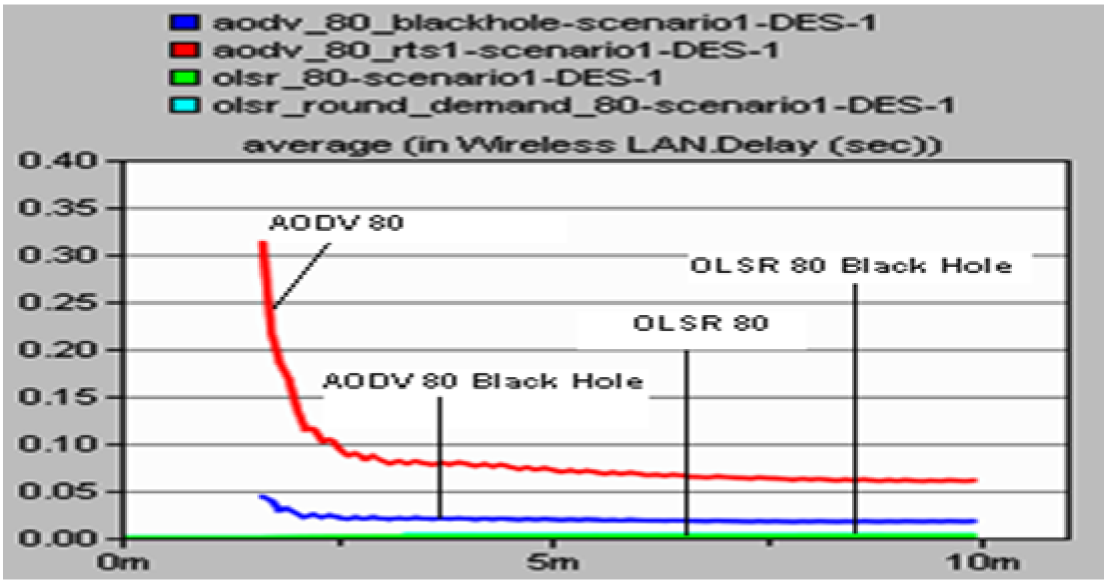

Fig.4. Delay for Low Density Network Black Hole Attack

verification functional area. This area is the core of network layer security module. Fourth, data processing area. This area feature is same to mac layer security module for packets discarded or forwarding.

CONCLUSION

Consider the following attributes: availability, confidentiality, integrity, authentication, authorization and non-repudiation. Several security mechanisms and protocols have been designed and proposed for mobile ad hoc networks. Key management is the central aspect of the security of mobile ad hoc networks, and it is still a weak point. In this thesis we propose a key management scheme, SEKM, which creates a PKI structure for this type of network in mobile ad hoc networks. Wireless sensor networks are being deployed in wide variety of applications, including military tracking and security is a vital requirement for these networks. Security protocols need key management schemes to establish secret keys between communicating parties. This thesis investigates and evaluates the most important key management schemes in wireless sensor networks. Namely, single network-wide key scheme, pair wise key establishment scheme, random key predistribution, and Q-composite random key predistribution schemes are explained. Extensive simulation results and comparisons are presented. The results show that random key predistribution schemes are the most suitable key management protocols for wireless sensor networks in terms of performance and security. Our future research directions involve comparing more key management schemes using different metrics and larger network sizes.

REFERENCES

[1] Mariano Garcıa Otero, Adrian Poblacion-Hernandez, “Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques”, International Journal of Distributed Sensor Networks, 2012.

[2] D.Devi Aurna, P.Subashini,Phd, SNAuth-SPMAODV:” Secure Neighbor Authentication Strict Priority Multipath AODV against Denial of Serviceattack for MANET in Military Scenario”, International Journal of Computer Applications , 2012.

[3] Dr.G.Padmavathi1, Dr.P.Subashini, Ms.D.Devi Aruna, “DSSS with ISAKMP Key Management Protocol to Secure Physical Layer for Mobile Adhoc Network”, International Journal of Network Security & Its Applications (IJNSA), 2012.

[4] H.C. Chaudhari, L.U. Kadam, “Wireless Sensor Networks: Security, Attacks and Challenges”, International Journal of Networking, Volume 1, 2011.

[5] Shahid Raza, Tony Chung, Simon Duquennoy, Dogan Yazar, Thiemo Voigt, Utz Roedig, “Securing Internet of Things with Lightweight IPsec”, SICS, 2011.

[6] T.Kavitha, D.Sridharan, “Security Vulnerabilities In Wireless Sensor Networks: A Survey”, Journal of Information Assurance and Security, 2010.

[7] Akyildiz I. F, Vuran M. C., “Wireless Sensor Networks”, John Wiley & Sons Ltd., (2010).

[8] Alfawar, M. Z., Alzoubi, S. 2009. A Proposed Security Subsystem for Ad Hoc Wireless Networks.In International forum on Computer Science technology and Applications. (2009), 1-4.

[9] Ammari H. M., “Challenges and Opportunities of Connected k-Covered Wireless Sensor Networks From Sensor Deployment to Data Gathering”, Studies in Computational Intelligence, vol. 215, Springer, (2009).