ISSN 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2012

# Security Requirements in Mobile Ad Hoc Networks

Mrs.V.Umadevi Chezhian[1], Dr. Ramar[2] , Mr.Zaheer Uddin Khan[3]

College of Business and Economics, Asmara, State of Eritrea[1],
Einstein Engineering College, Tirunelveli, India[2],
Lecturer in Mathematics, Eritrea Institute of Technology(E.I.T), Asmara Eritrea [3]

***ABSTRACT:*** ***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. Security is a basic and paramount requirement for an ad hoc network because of its intrinsic vulnerabilities in order for users to perform protected peer-to-peer communication over multi-hop wireless channel. Depending on the application context, a user may desire various security services such as authentication, integrity, non-repudiation, Confidentiality, Key and Trust Management and access control. Unlike wired networks that have dedicated routers, MANET has infrastructure-free network where the MNs themselves perform basic network function as a router and packet forwarding. Therefore, security in MANETs is a pressing issue, which needs immediate research attention.***

Key words*: MANET, Security, Authentication, Integrity, Non-repudiation, Confidentiality, Key and Trust Management, and Access Control.*

## 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. Ad hoc networks 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. 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. 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 [1]. 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 [2]) or IPv6 auto-configuration[3] or even randomly (e.g., Zero-Configuration [4]. 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. It is expected that a single organization will undertake the deployment and administration of these networks. 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 [5]. An approach that has similarities but targets a more general setting proposes a key management scheme for sensor networks [6]. 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) [7]. 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.

ISSN 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2012

## II. 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-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.

## IV. 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.

## V. 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. 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.

*A. Trust model:* it must be determined how much different elements in the network can trust each other. The environment and area of application of the network greatly affects the required trust model. Consequently, the trust relationships between network elements affect the way the key management system is constructed in network.

*B. Trust third party (TTP):* [8] a centralized authority (e.g., a key distribution center [KDC] or certification authority [CA]) is trusted by every entity and an entity A is trusted by another if the authority claims A is trustworthy. This schemes is centrally managed, thus the neighborhood of the central point is potentially the bottleneck of a scalable network and subject to DoS attacks.

*C. Web-of-trust:* There is [9] no particular structure exists in such trust graphs. Each entity manages its own trust based on direct recommendation from others. The scheme is fully distributed, making it resilient to attacks, but also difficult to achieve consensus among various entities.

*D. Localized trust:* [10] this model is the middle ground of the previous two graphs. A node is trusted if any k trusted entities among the node's one-hop neighbors claim so, within a bounded time period. As trust management and maintenance are fully distributed in space and time domains, the model fits in large dynamic ad hoc networks with mobility and on-demand authentication requirements.

*E. Cryptosystems:* available for the key management: in some cases only public- or symmetric key mechanisms can be applied, while in other contexts *Elliptic Curve Cryptosystems* (*ECC*)are available. While public-key cryptography offers more convenience (e.g. by well-known digital signature schemes), public-key cryptosystems are significantly slower than their secret-key counterparts when similar level of security is needed. On the contrary, secret-key systems offer less functionality and suffer more from problems in e.g. key distribution. ECC cryptosystems are a newer field of cryptography in terms of implementations, but they are already in use widely, for instance in smart card systems.

## VI. 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 ad hoc networks 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. 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. 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).

If public-key cryptography is applied, the whole key. Consequently, as the physical security of nodes may be

ISSN 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2012

poor, private keys have to be stored in the nodes confidentially, for instance encrypted with a system key. For dynamic ad hoc networks this is not a wanted feature and thus the security of the private key must be guaranteed with proper hardware protection (smart cards) or by distributing the key in parts to several nodes. Hardware protection is, however, never alone an adequate solution for preventing attacks as such. In ad hoc networks a centralized approach in key management may not be an available option, as there may not exist any centralized resources. Moreover, centralized approaches are vulnerable as single point of failures. The mechanical replication of the private keys or other information is an inadequate protection approach, since e.g. the private keys of the nodes simply have then a multiple possibility to be compromised. Thus a *distributed approach* in key management for any cryptosystem in use - is needed, as proposed e.g. in [11] (Zhou *et al.*, 1999).

## VII. THRESHOLD CRYPTOGRAPHY

Often, the sender/receiver is an organization. The goal of threshold cryptography (TC) is to split a cryptographic operation among multiple users so that some predetermined number of users can perform the desired (cryptographic) operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and/or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key. The power to sign should then be shared, to avoid abuse and to guarantee reliability. The goal of TC is to make this possible. The basic idea is as follows: a cryptofunction*g* is homomorphic, i.e.,

$$gb(k1+k2) = gb(k1)*gb(k2)$$

where b is the input message, and k belong to key space, k= k

Both RSA and ECC are homomorphic. Therefore, threshold cryptography is applicable and cryptographic operations can be split among multiple users such that any subset comprising of *t* users can perform the desired operation, where *t* is a predefined number. In a *t* out of *n* scheme, any set of *t* users can perform the desired operation, while any set of (*t*1) users or less cannot. A cryptographic scheme based on threshold cryptography is secure against an attacker as long as the attacker compromises no more than (*t*-1) nodes.

*A. Key creation*: it must be determined which parties are allowed to generate keys to themselves or other parties and what kind of keys.

*B. Key storage*: in ad-hoc networks there may not be a centralized storage for keys. Neither there may be replicated storage available for fault tolerance. In ad-hoc networks any network element may have to store its own key and possibly keys of other elements as well. Moreover, in some proposals such as in [11](Zhou *et al.*, 1999), *shared secrets* are applied to distribute the parts of keys to several nodes. In such systems the compromising of a single node does not yet compromise the secret keys.

*C. Key distribution*: the key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be distributed so that confidentiality, authenticity and integrity are not violated. For instance whenever symmetric keys are applied, both or all of the parties involved must receive the key securely. In public-key cryptography the key distribution mechanism must guarantee that private keys are delivered only to authorized parties. The distribution of public keys need not preserve confidentiality, but the integrity and authenticity of the keys must still be ensured.

## VIII. ACCESS CONTROL

Access control consists of the means to govern the way the users or virtual users such as operating system processes (*subjects*) can have accesses to data (*objects*). In networking, access control can e.g. involve the mechanisms with which the formation of groups of nodes is controlled. Only authorized nodes may form, destroy, join or leave groups. Access control can also mean the way the nodes log into the networking system to be able to communicate with other nodes when initially entering the network. There are various approaches to the access control:

*A. Discretionary Access Control (DAC):* DAC offers the means for defining the access control to the users themselves. DAC allows the restriction of access to objects based on the identity of subjects or groups of subjects.

*B. Mandatory Access Control (MAC):* MAC involves centralized mechanisms to control the access to objects with formal authorization policy. DAC and MAC are often applied together so that DAC allows the system user subjects to control access of other subjects, while MAC controls and restricts the operation of DACs in the system in general. This

kind of approach prevents the system from failures generated by the actions of careless users.

*C. Role Based Access Control (RBAC):* RBAC applies the concept of *roles* within the subjects and objects. In RBAC systems subjects can have several roles of which one is at a time active and therefore the accesses to objects are defined with respect to roles, not subjects. As stated in, RBAC does not necessarily involve the controlling of access to information only, but also the restriction of access to *functions* within the system. Thus roles are group oriented sets of *transactions* associated to roles that the specific users can perform to given objects. For example, in banking applications using RBAC users with different roles may have the same set of accesses to the same objects as such, only with different limits in the amount of transferable money. In DAC and MAC systems these kinds of definitions could not be directly are applied.

## XI. CONCLUSION

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. 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. All security mechanisms applied in networking more or less require the use of cryptography, which on the other hand implicates a strong demand for secure and efficient key management mechanism. Access control needs to exist a method for restricting the access of foreign nodes to the network, which requires the use of a proper authentication mechanism. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for security mechanisms.

## REFERENCE

1. Ha Duyen Trung, Watit Benjapolakul, Phan Minh Duc, "Performance evaluation and comparison of different ad hoc routing protocols", *Science Direction*, Computer Communications 30 (2007) , 2478–2496.
2.Droms .R, "Dynamic host configuration protocols", *IETF RFC* 2131, 1997.
3. Thomson .S, Narten .T, , "IPv6 stateless address autoconfiguration", *IETF RFC*, 1971.
4. Hattig .M, 2001, Ed., *Zero-Conf IP Host Requirements*, Draftietfzerofonf-reqts-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 alternate path routing for load balancing in mobile ad hoc networks", Mobi HOC, 2000.
9. Zimmermann .P, The Official PGP User's Guide, MIT Press, Cambridge, MA, 1995.
10. Luo .H, Zerfos .P, Kong .J, Lu .S, and Zhang .L, 2002, "Self-securing ad hoc wireless networks", Proceedings *of the IEEE International Symposium on Computers and Communications* (ISCC), Taormina, Italy, 2002.
11. Zhou .L and Haas. Z, "Securing ad hoc networks", *IEEE Network Magazine*, vol. 13. 1999.

## BIOGRAPHY

***V.Umadevi Chezhian*** is doing various research activities. She published articles and research papers in reputed international journals. She had good teaching experience in Arulmigu Palaniandavar Arts and Science College for Women, India, Cyryx Information Technology in Male, Republic of Maldives and currently working as a lecturer in the College of Business and Economics, University of Asmara, State of Eritrea. Her qualification is M.Sc., (CS & IT), M.Tech (IT), M.Phil, (Computer Science), D.C.S., (Diploma in Computer Software), and submitted her PhD. She is interested in Research activities related to wireless communication and network security.

***Dr. K. Ramar***, Principal and Einstein Engineering College, Tirunelveli. Tamilnadu, India. Recognised guide in Manonmaniam Sundaranar University, Anna University in Chennai and Tirunelveli , Mother Teresa University, Alagappa University and Dravidian University inAndra Pradesh. Visited abroad Japan, Malaysia for various internaltional conferences. Expert member of Acted and Affiliation Committee member to affiliate colleges under Anna University. Senate member in Manonmanium Sundaranar University. Board of studies member for various colleges in India. He published two books. He has given Radio talks and involved in Guest lecturer activities. He has organized many Conferences. Technical committee member of Wasada University, Japan.

**Zaheer uddin Khan**, Lecturer in Mathematics, Eritrea Institute of Technology (E.I.T), having overall academic experience of more than 12 years of purely college level

teaching to undergraduate students of Universities of PAKISTAN and ERITREA as well as he has being remained part and parcel of not only taking and accepting the challenging courses but also gave a firm stand to the Department by improving ,standardizing, updating the course outlines and curriculum to the international level as a team effort in the curriculum design committee in EIT. He is working on different projects and research activities such as organizing the Manuscripts of Engineering Mathematics book, Mathematics Lecture notes on different courses like Introduction to General Topology and Number theory, which is the base for the application and use of Cryptography for security issues in different areas of Computer Networking Mobile/wireless communication etc.

He is always happy to work together as a Team under the umbrella of learning and research-enriched environment of any institute to promote and discover his hidden research potentials and capabilities.