www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1384-1393

A SURVEY ON SECURITY IN MOBILE ADHOC NETWORK

Dr. Anna Saro Vijendran , A. Kamatchi,
Director of MCA, SNR & Sons College, Coimbatore.
Ph.D Scholar, Department of Computer Science, Karpagam University, Coimbatore

Abstract

Today, the popular technology in Networking talks about MANET(Mobile Adhoc Network). It makes tremendous change in wireless network. A mobile adhoc network is an wireless network connected with autonomous mobile nodes which are self configured and dynamic. Security is a main concern for protecting the communication between mobile nodes. The security design of the mobile adhoc network leads many problems such as shared wireless medium,, severe resource constraints, and highly dynamic network environment. In this paper we identify the security issued relevant to this problem, analyze the challenges to security design, and evaluate the state-of-art security proposals etc. The security solution is given according to the survey.

Keywords: MANET, MANET Security, Mobile Security, MANON.

1. INTRODUCTION

Mobile adhoc network is an wireless network connected with autonomous mobile nodes which are self configured and dynamic.

Mobile Adhoc Network

Security Solutions for Layers:[1]

Layer	Security issued
Application Layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

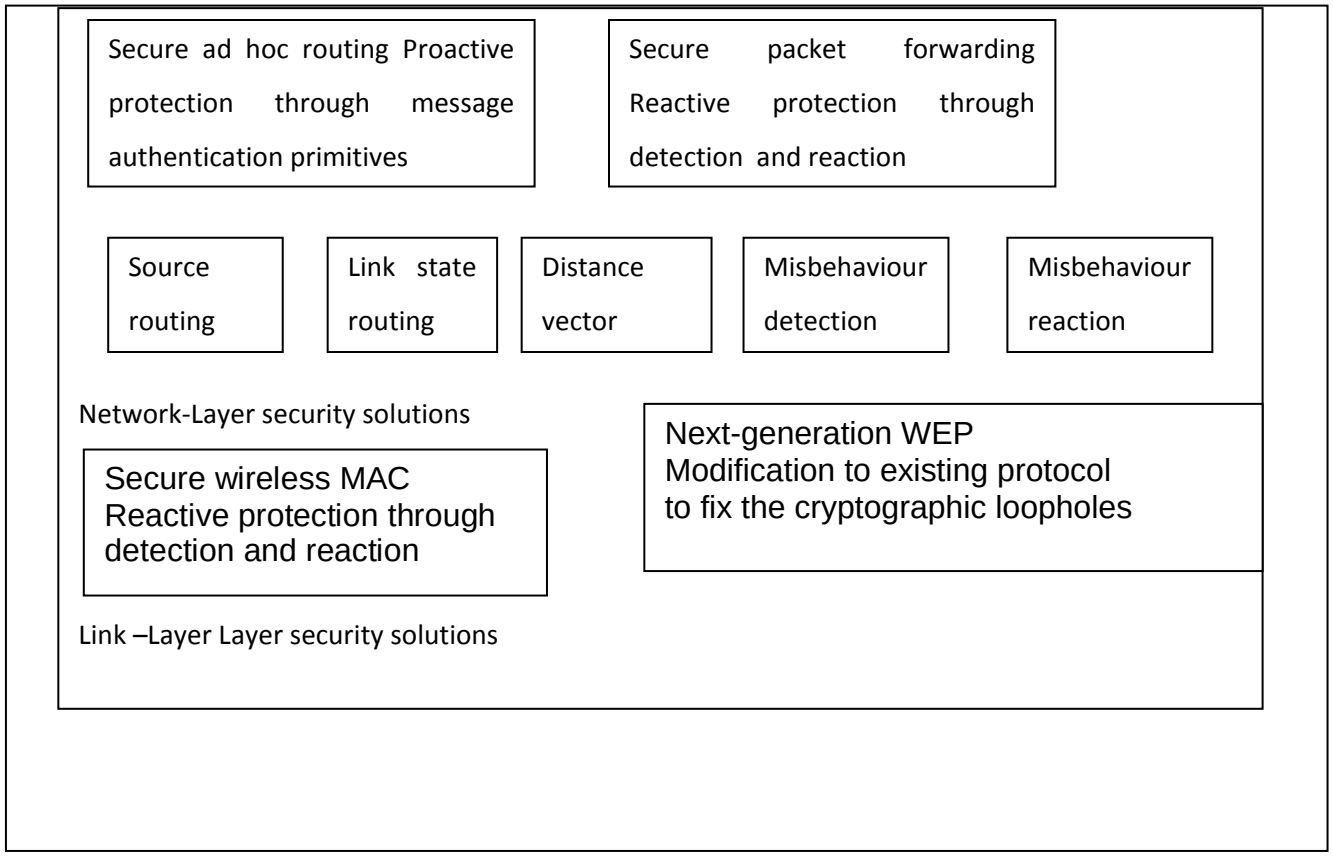

Fig1. Components of Security solutions

In Table1[1]the author shows that security solutions for each layer. From Figure[1] the author shows that components of security solutions.

2. ATTACK TYPES IN MOBILE AD HOC NETWORKS

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types.[2]

(i). **External attacks,** in which the attacker aims to cause congestion, spread fake routing information or disturb nodes from providing services.

(ii). **Internal attacks,** in which the opponent needs to gain the normal access to the network
and contribute the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a
basis to conduct its malicious behaviors.

2.1. Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. In the practice, the attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

2.2. Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network .As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

2.3. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks.

The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

3. SECURITY CRITERIA

Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

3.1. 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. [3]This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.[4]

3.2. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways.

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an opponent 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.

3.3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

3.4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators.[3] 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. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

3.5. Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

3.6. 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. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

3.7. Anonymity

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

Security Criteria: Summary

We have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network. Moreover, there are some other security criteria that are more specialized and application-oriented, which include location privacy, self-stabilization and Byzantine Robustness, all of which are related to the routing protocol in the mobile ad hoc network. Having dealt with the main security criteria, we then move to the discussion on the main threats that violate the security criteria, which are generally called as attacks.

4. SECURITY SCHEMES IN THE MOBILE AD HOC NETWORKS

In the previous subsection, we have introduced several well known attack types in the mobile ad hoc network. Therefore, it should be an appropriate time now to find some security schemes to deal with these attacks. In this part, we discuss several popular security schemes that aim to handle different kinds of attack listed in the previous subsection.

4.1. Intrusion Detection Techniques

Intrusion detection is not a new concept in the network research. According to the definition in the *Wikipedia*, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [5]. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details.

4.2. Intrusion Detection Techniques in MANET: the First Discussion

The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al.[6] In this paper, a general intrusion detection framework in MANET was proposed, which was distributed and copperative to meet with the needs of MANET. The proposed architecture of the intrusion detection system is shown below in Figure 2.

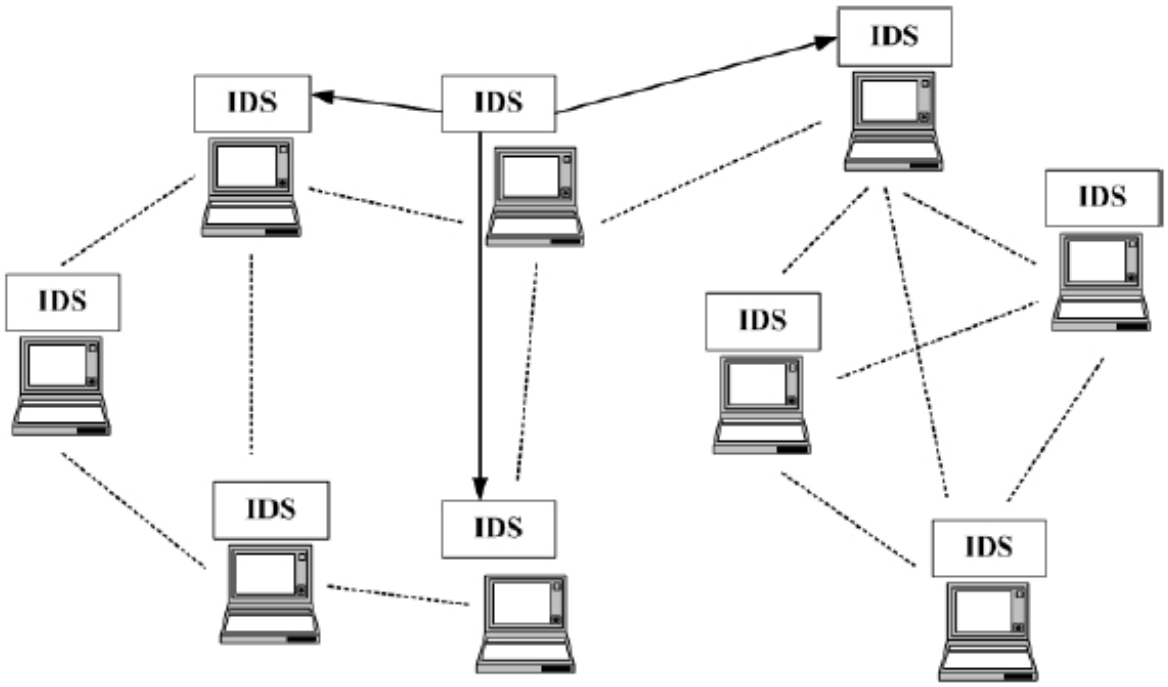

Fig 2. An IDS Architecture for MANET

In the conceptual model, there are four main functional modules:

Local data collection module, which mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.

Local detection engine, which examines the local data collected by the local data collection module and inspects if there is any anomaly shown in the data. Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviors and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviors based on the deviation between the current observation data and the normal profiles of the system.

Cooperative detection engine, which works with other IDS agents when there are some needs to find more evidences for some suspicious anomalies detected in some certain nodes. When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighboring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbors by some selected algorithms such as a distributed consensus algorithm with weight. Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.

Intrusion response module, which deals with the response to the intrusion when it has been

confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behavior varies with the different kinds of intrusion.

5. SECURITY SOLUTIONS FOR MANONS(MOBILE ADHOC NETWORK OF NETWORKS).

To aid the application of MANoN in any wireless environment, when required, and to achieve the services demanded by the user, we need to define MANoN as a whole object with clear syntax and semantics[7]. In this section, the author present a framework scenario that can be applied to MANoN in different network environments, for example cellular systems, smart homes or military. Figure 3 depicts four MANETs, each network is a legacy under its own management and policies coming together to create a MANoN, each MANET has the ability of performing separately which, enables it to disconnect and join without effecting the main MANoN system. Networks 1, 2 and 4 are pre-defined and connected to exchange PKI information (Public keys P, Private keys pr) whereas, the undefined network is obviously not. Nodes in each MANET are classified into: *General Node (GN)* **r**egular ground nodes are typically soldiers equipped with communication and computation limited devices, *and Back-Bone Node (BBN)* they are usually special units, such as tanks and personnel carriers, which have more extensive facilities than regular ground nodes. BBN nodes will carryout CAs (Servers CAs and Combiners CAc) duty.[8]

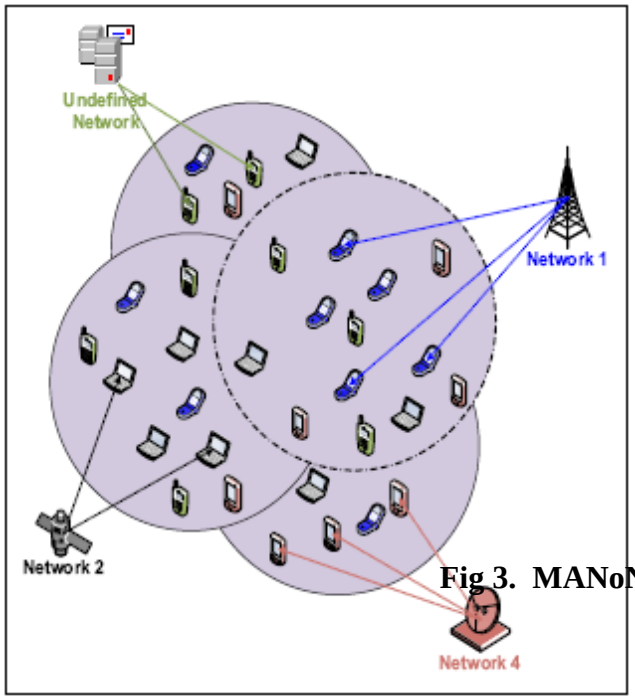

Fig 3. MANoN Scenario

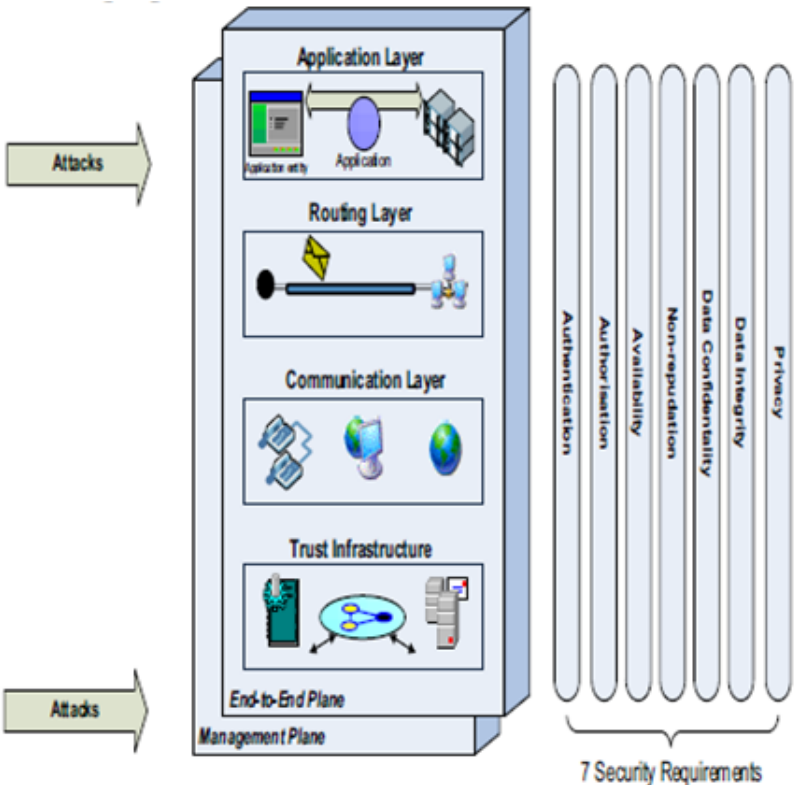

Fig.4. MENoN security Architecture

5.1 Security Layers

In order to provide a comprehensive solution, we divide our complex MANoNs logically into separate architectural components. This separation allows a systematic approach to the MANoNs that can be used in the planning of new security solutions for the security threats our system might face as well as for assigning security to existing MANoNs. Moreover, the success of the OSI [9] model applied in designing network protocols is a good example to follow in designing security protocols. A layered architecture can provide such advantages as modularity, simplicity, flexibility and standardization of protocols. There security mechanisms.

***Communication*:** The communication security layer consists of the transmission facilities protected by the security requirements, as well as the security mechanisms applied to data transmitted between nodes.[11]

are four security layers for MANoNs, which are built on one another to provide a network-based solution. The functionality of each layer is explained below.

***Trust Infrastructure*:** The trust infrastructure security layer represents a fundamental building block of the network, consisting of the basic relationships between the nodes. An example is given by the explanation of Zhou and Hass[10] of a well-deployed PKI environment (threshold cryptography), as there is no centralized certification authority in which public and private keys are exchanged between all nodes. The security association established in the trust infrastructure layer must serve the upper layer

***Routing*:** The routing security layer consists of basic transports and connectivity as well as the individual nodes; since each node in the ad hoc network acts as host and router, our MANoN is not different from that perspective.

Moreover, nodes must exchange information about their neighbours to construct the network topology

in order to apply one of the ad hoc routing protocols (Proactive, Reactive and Hybrid).[12]

Application: The application security layer concentrates upon the security of the network-based services and network protocols that perform sub-network access operations from end system to end system which, are applied in our MANoNs [13]. After dividing our security architecture into four layers, consider two distinct security planes, the ***Management Plane*** **and the** ***End-to-End User Plane,*** which are protected by our security requirements from any threats and attacks.

Management Plane: The management security plane supports FCAPS (Fault-management,Configuration, Accounting, Performance and Security)[13][14]. Moreover, it is concerned with the protection of OAM&P (Operation, Administration, Maintenance and Provisioning)[15] functions of the nodes, services and applications.

End-to-End user Plane: The end-to-end user plane deals with end-user data flow (information flow) and security mechanisms related to the end users of the system[16].

6. SIMULATION RESULTS

This section will show the results of providing Authentication and Authorisation certificates to nodes of our MANoN system. NS-2 simulations have been carried out to evaluate the predefined scenario. The parameters used for this simulation is depicted in table 2.

NS-2 Simulation Parameters

Total no.of nodes	10,20,40,60
No. of BBN (CA)	4,10
Network area	100 m * 1000 m
Total simulation time	500 s
Type of Routing	AODV
Radio range	250 m
Max node speed	1,10,15,20,25,30
Pause Time	0,10,40,60,100
Antenna model	Omni Antenna

Table 2

Success ratio is one of the most significant factors that measures the number of successful certificate authentication and authorization requests to the total number of
certificate authentication requests that take place during the simulation time. As an assumption, each node will make at least one authentication request. Therefore, the total number of authentication requests made during the simulation time is equal to the number of nodes trying to enter the MANET.

Fig. 5 shows the success ratio against mobility and network size. Mobility is most often a big issue in developing ad hoc protocols. As can be seen, our MANoN is not much affected by mobility. In general, the success ratio increases with high mobility situations and large network sizes. The effect of mobility is more noticeable with a small number of nodes.

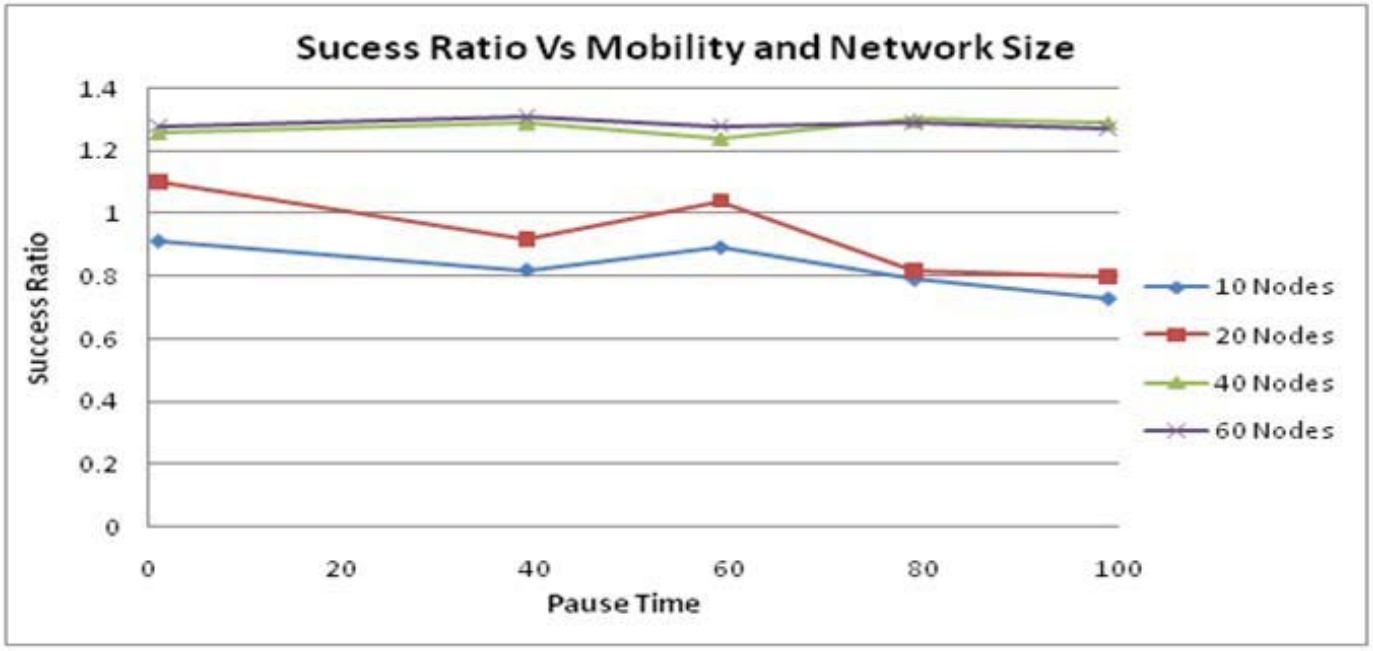

Figure 5. Success Ration Vs Mobility and Network Size

CONCLUSION

This survey has presented the best known protocols for securing the routing function in mobile ad hoc networks. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. The comparison we have completed between the surveyed protocols indicates that the design of a secure adhoc routing protocol constitutes a challenging research problem since already existing generic solutions, such as IPsec, cannot be successfully applied. Additionally, the flexibility of ad hoc networks enables them to be deployed in diverse application scenarios. Each different scenario has its own set of security requirements and places unique demands on the underlying routing protocol.

Hence, an additional difficulty in designing a secure protocol lies in the application scenario that is going to be protected, and how well the protocol can handle scenarios different than the scenario for which it has been designed. Military applications of ad hoc networks are probably the area that requires the most highly secure routing functionality . In this case the applications that run on top of the network are of critical importance, therefore the underlying routing process should provide a high level of protection, while possibly having less strict performance requirements. On the other hand, commercial application scenarios of ad hoc networking may place higher demands on the underlying routing protocol.

However, security still plays an important role since even in commercial or domestic ad hoc environments the exchanged information is usually confidential, e.g. credit card numbers, or of a private nature. Therefore, a flexible secure ad hoc routing solution should take into account the performance security trade-off associated with an application and dynamically achieve the required equilibrium. An example of the routing challenges currently faced by mobile ad hoc networks is outlined in a previous review paper . Although the authors mention challenges such as quality of service support and location-aided and power-aware routing approaches, there is no mention of security considerations.

References:

1. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, Ucla Computer Science Department," Security in Mobile Adhoc networks:challenges and Solutions", IEEE Wireless Communications • February 2004.
2. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *AdHoc Networks Technologies and Protocols (Chapter 9)*, Springer, 2005.
3. Amitabh Mishra and Ketan M. adkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30)*, CRC Press LLC, 2003.
4. Lidong Zhou and Zygmunt J. Hass, \ Securing Ad Hoc Networks, *IEEE Networks Special Issue on Network Security*, November/December 1999.
5. Intrusion-detection system, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Intrusion-detection_system.
6. Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pages 275–283, Boston, Massachusetts, August 2000.
7. Ali H. Al-Bayatti, Hussein Zedan, Antonio Cau, Security Solution for Mobile Ad hoc Network of Networks (MANoN) Fifth International Conference on Networking and Services,2009.
8. L. Zhou, and Z. J. Haas, "Securing ad hoc networks", IEEE, 1999, pp. 24-30.
9. E. Carrieri, C.A. Rocchini, A. Fioretti, and A.J. Haylett, "An OSI compatible architecture for integrated multichannel metropolitan and regional networks", Integrating Research, Industry and Education in Energy and Communication Engineering, MELECON '89. Mediterranean, 11-13 April, 1989, pp. 639 – 643.
10. L. Zhou, and Z. J. Haas, "Securing ad hoc networks", IEEE, 1999, pp. 24-30.
11. ITU-T Recommendation M.3010, "Principles for a Telecommunications management network", February 2000.
12. Perkins C.E., Royer E.M., "Ad-hoc on-demand distance vector routing Mobile Computing Systems and Applications", Proceedings. WMCSA'99. Second IEEE Workshop on, 25-26 Feb. 1999, pp: 90 – 100.
13. ITU-T Recommendation M.3400, "TMN Management Functions", February 2000.
14. R. Boutaba, and A. Polyrakis, "Projecting FCAPS to Active Networks", Enterprise Networking, Applications and Services Conference Proceedings, 2001, pp. 97 – 104.
15. S. Hayes, "A standard for the OAM&P of PCS systems", personal Communications, 1994, pp.24.
16. ITU-T Recommendation X.701, "Information technology – Open Systems Interconnection - Systems management overview", August 1997.