International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12-13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

Review paper on Security Mechanism for Supporting Routing Services on WANET

Ashwini Shendre[1], P. S. Mohod [2]
[1,2]Department of Computer Science & Engineering,, G.H.R.I.E.T.W., *Rashtrasant Tukdoji Maharaj Nagpur University Nagpur, India*

ABSTRACT—
Increases the dependence of people on critical applications in wireless networks, high level of reliability, security and availability to ensure secure and reliable service operation. The use of SAMNAR (Survivable Ad hoc and Mesh Network Architecture) to design a path selection scheme for WANET routing and using the concept of SG-PKM (survivable public key infrastructure) uses groups based on users relationships to increase survivability in the presence of different types of attacks. Finally, it highlights open issues in designing survivable key management Systems. SG-PKM technique also improves the network performance and survivability. Result shows under any condition and attack the survivability is archived in routing services.

Keywords— Security management, wireless ad hoc networks, survivability, routing.

I. INTRODUCTION

Recent technological advances the use of portable devices in wireless networking which popularized them, for executing anywhere and anytime critical applications the peoples are mostly dependent on portable devices , like business-critical applications in financial transactions or life-critical applications in healthcare. Such dependant behaviour claims simultaneously for high level of reliability, security and availability to assure both secure and reliable service operation even under failures, intentional threats or accidents .The Wireless Adhoc Network will support to universal computer connectivity through the self organized portable devices (nodes) and multi hop network by using some self organized technique .

Various security issues have in critical application , because of this reason they are not in focus .For improve this use some important parameters which need to consider and make the design with them such as self organization which increase the complexity of security management operation as access control, node authentication, secure routing ,cryptographic key distribution, survivability [1][3].This all parameters affect directly on to the network parameters. The aim of proposed system is to increases the survivability and network performance's use SAMNAR (Survivable Ad hoc and Mesh Network Architecture) along with the one technique which helps us to increase the survivability. The main concept of the survivability is that when the two nodes or network were communicating with each other that time if some attacker want to hack the important data of that link this proposed mechanism were producing the security over there. Its goal lies in managing adaptively preventive, reactive and tolerant security mechanisms to provide essential services even under attacks, intrusions or failures .

The SAMNAR is design a path selection scheme for WANET routing. SAMNAR manages preventive, reactive and tolerant security mechanisms in an adaptive and coordinated way. It support to focusing on the survivability of link-layer connectivity, routing and end-to-end communication. This SAMNAR provides the best path selection scheme on the basis of distance measure. The distance is small that path is best for transaction or processing. SAMNAR is only best for selecting the path selection scheme. It provide a low rate of survivability. This is a drawback of SAMNAR. To improve this drawback use the one technique along with the SAMANR i.e. SG-PKI (survivable public key infrastructure) . SG-PKM is basically used to focus on survivability increase in routing services on WANET. This whole mechanism is gives the high level of secure routing services.

II. RELATED WORK

In REP(recommendation exchange protocol) have the trust relationship concept, it means trust relationship between two nodes on the basis of previous individual experiences and on the recommendations of others .Here uses the certification concept so no use of any type of recommendation. And trust is based on certificate verification. SABER and SITAR this two Survivability concepts have been initially created for survivability who used to focuses on to the survivability and independence criteria. They had been provided the integration of security mechanism to improve security. But this two architecture was supported to single criterion based type .Survivability concept applied in wireless and mobile networks. Existing works can be categorized in two classes, those to improve network survivability managing mechanisms for tolerating faults and those that propose security management architectures to survive intrusions and attacks . Creating a best group ultimately it achieves the survivability In a security management architecture towards a survivable access control in WANETs is proposed. It is very harmful, attacker attack on WLAN on access point, to improve WLAN survivability this mechanism is defined. security management architectures for survivable wireless sensor networks have been designed, focusing on DoS attacks and on multiple attacks, respectively. However, all those architectures handle only one specific service and do not employ more than two defense lines together, being still unable to attain simultaneously all survivable properties, as resistance, recognition, recovery and adaptation[1]. Survivability mechanisms for multihop wireless networks: proactive and reactive protection only used . A number of simulations to evaluate the performance of the Recommendation Exchange Protocol and show its scalability. We show that our implementation of the REP protocol can significantly reduce the number messages.

We also present other results that indicate that our model detects behavior changes of nodes and is robust to slander and colluding attacks. The results reveal that the proposed model tolerates up to 35% of liars. We also evaluate our model in mobile multihop ad hoc networks. We show the effectiveness of the relationship maturity parameter, which reduces the trust level error by almost 50%, in certain cenarios. Future work includes defining and implementing a monitoring scheme for a specific application and applying our
model to improve the service/application performance, as for
instance, an authentication protocol [5].

III. TECHNOLOGIES

A. SAMNAR(Survivable Ad hoc and Mesh Network Architecture)

The SAMNAR, Survivable Ad hoc and Mesh Network
Architecture, is inspired on the human body immune system.

It defines a three security management approach by the adaptive coordination of preventive, reactive and tolerant defense lines. Preventive defense lines include security mechanisms tries to avoid attacks, such as firewall ,cryptography, and access control techniques. Reactive
defense lines try to detect and react against intrusions by security mechanisms, such as intrusion detection systems. And reputation systems.

Tolerant defenses aim is to decreases the damages caused by attacks or intrusions, and recover compromised services. When recovery reaches the Redundancy techniques is also introduced in system. SAMNAR mainly focuse on supporting the development of essential services, as link-layer connectivity, routing and end-to-end communication. It establishes three integrated modules: **survival**, **communication** and **collect**. Each node/device in the network independently implements and performs these three modules, reform them to consider its resource limitations. SAMNAR was designed to work in a distributed way, however it can be easily modified to work in a centralized way.

The **survival module** holds five independent components. Four of them are work on a resistance, recognition, recovery and adaptability, and the last one is the control component. These properties have important role to represent the network capability of remove attacks; detecting attacks and evaluating the extent of damage; keeping track of all disrupted information or functionalities; and quickly incorporating lessons learned from failures and, thus, adapting to emerging threats.

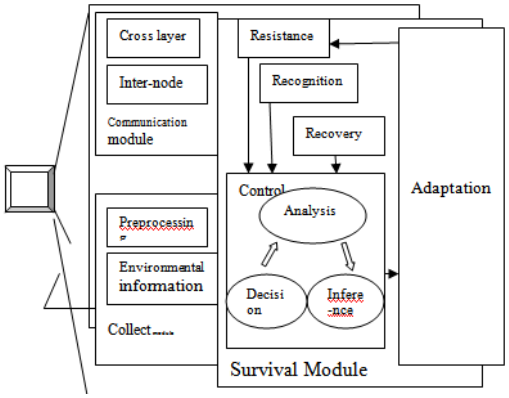

Fig.1 SAMNAR architecture

The **resistance component** contains the preventive mechanisms, such as firewall, access control, authentication and cryptography . Depending upon the network and environmental condition the preventive mechanism and their configuration will be changes ,on this condition the component works in a self-protection and self adjusting fashion . Always the simple rules of firewall can be applied in more secure environment , but sometimes the rule of a distributed firewall, can be more difficult in certain environments. Another example is the cryptographic key size used that can be larger depending on the environment or network condition.

The **recognition component** incorporate with reactive mechanisms to identify malicious behaviors, such as IDSs, reputation systems, anti-malwares and anti-spammers. Recognition mechanisms can have the capability to stopping intrusions and reacting against intrusions .In the adaptation component all the mechanisms selected for reconfigured if necessary New configurations on the fly, such as IDS rules, depend on the network and environment conditions. Also, this component provides information about detections, trustworthiness of neighbor devices, among others to the control component.

The **recovery component** consists of tolerance mechanisms , enhance the attack tolerance of network essential services. Mechanisms to restore disrupted information or functionality, such as replication or redundancy, have been employed as tolerant mechanisms. For example, the use of two cryptography algorithms successively and the replication of message pieces. Sending redundant message pieces by different routes increases the probability of the message to be received by the destination node and the possibility of message recovery in case of piece losses. However, redundant strategies employed must consider resource limitations, as well as service and application requirements

The **adaptation component** enclose the previous ones. It is responsible for adapting preventive, reactive and tolerant mechanisms, as well as local or network configurations. It can make the replacement of a given protocol or a defense mechanism, such as applying the stronger one with changing a weaker cryptographic algorithm depending on the requirements on time. Further, this component can change the key size of a cryptographic algorithm, the rules into an IDS or a firewall, the used route and others in accordance with the network condition or decisions taken by the control component.

The **control component** manages and coordinates all modules in the architecture. It receives information from collect modules and communication modules ,also from the resistance, recognition and recovery components. Its purpose is to make inference and decision by correlating and analyzing all information . All decisions send to the adaptation component that defines and updates parameter values of other modules or components. Adaptation component learns with taken actions keep track and later , if the node or network presents a similar condition. it can take the same action.

The **communication module** is responsible for cross-layer and inter-node communications. The **inter-layer component** offers the exchange of information in between two different network means inter-layer . It supplies information from different network layers to the control component, hence, it takes decisions based on all network layers and achieves the survivability for all of them. The **internode component** provides the communication, exchange and synchronization of information among the nodes aiming to guarantee the survivability of the whole network. For example, the information of the node configuration or network intrusion detections. The **collect module** holds mechanisms to gather all data required by the survival module. This module is composed of the *preprocessing* and *environmental information* components. The first one is exploited when gathered data need to be processed before sending to the survival module. Normalizations, previous calculations and others are examples of preprocessing used to facilitate analyses and inferences of the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required[1].

B. Survivable key management system

SG-PKM include small groups called initiator groups (IGs), which consist of nodes whose users have a friend relationship among them. All nodes in a group have the same role without cluster heads. Groups are essential for joining a new node to the system, issuing certificates, and renewing keys. However, the maintenance of IGs is not critical, since it is designed in order to self-adjust to changes, and also to minimize the computational cost in maintaining groups and the network overhead.

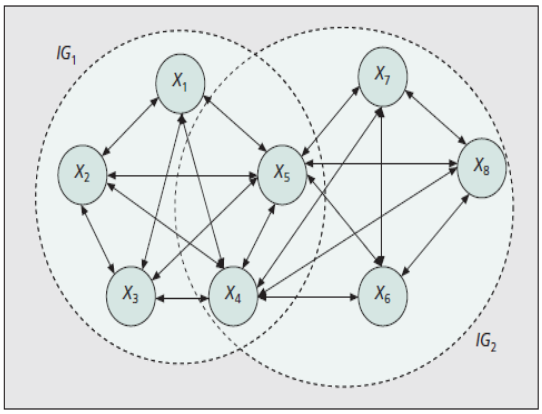

Fig.2 Initiator Groups IG1 and IG2

Figure 1 illustrates two initiator groups, *IG*1 and *IG*2. *IG*1 is composed by *X*1, *X*2, *X*3, *X*4, and *X*5, and *IG*2 by *X*4, *X*5, *X*6, *X*7, and *X*8. The respective users owning the nodes in *IG*1 are friends as well as the users owning the nodes in *IG*2. Nodes into a group reciprocally issue public key certificates among them. These certificates are represented by the double arrows meaning the existence of certificates mutually issued between two nodes. The intersection between *IG*1 and *IG*2 by the nodes *X*4 and *X*5 is also represented. It is important to point out that nodes within a group are not necessarily physical neighbors. However, they must be able to communicate with each other even through a direct communication or by a routing protocol. Furthermore, all nodes might be mobile, and the routing protocol must deal with it. SG-PKM works with two types of certificates: *node* and *group* certificates. Node certificates bind user public keys with their identities and group certificates bind group public keys with group identification. A node certificates is signed with the private key of the group in which it participates. Group certificates are signed with the private key of other groups. provides an overview of SG-PKM in three layers: *network model*, *trust model*, and *group certificate graph*. The network model represents physical connections between nodes. The trust model represents the trustworthiness among nodes (i.e., if two nodes have exchanged their public keys, they have a friend relationship and a connection on the trust model)[2].

C. Certificate

The heart of the X.509 is the public key certificate associated with each user. These user certificate are assumed to be created by some trusted certification authority(CA) and placed in the directory by the CA or by the user. The certificate server itself is not responsible for the creation of public keys or for the certification function . Here uses the X.509 certificate.

IV. CONCLUSION

This work presented a survivable management architecture for ad hoc and mesh networks called SAMNAR. Its goal lies in making these networks able to provide essential services even in face of attacks and intrusions. SAMNAR is based on a coordinated integration among the preventive, reactive and tolerant defense lines, being able to self-adapt to different network conditions. In this increase the survivability and network performance using the self organized technique of survivability ie.SG-PKM.

REFERENCES

[1] Michele Nogueira, Helber Silva, Aldri Santos, and Guy Pujolle, "Security management architecture for supporting routing services on WANTE**"** IEEE Transactions On Network And Service Management, Vol. 9, No. 2, June 2012

[2] Michele nogueira, université pierre et marie curie Eduardo da silva, aldri santos, and luiz carlos ," Survivable Key Management On WANETS" IEEE Wireless Communications 2011 IEEE

[3] Osameh m. Al-kofahi and ahmed e. Kamal, " survivability strategies in Multihop wireless networks **"**IEEE Wireless Communications 2010 IEEE

[4] Michele Nogueira Lima, Aldri Luiz dos Santos, and Guy Pujolle," A Survey of Survivability in Mobile Ad Hoc Networks" IEEE communications surveys & tutorials, vol. 11, no. 1, first quarter 2009

[5] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model" IEEE transactions on network and service management, vol. 7, no. 3, september 2010

[6] Yi Qian And Kejie Lu, University Of Puerto Rico At Mayagüez David Tipper, "A design for secure and Survivable wireless sensor networks", IEEE wireless communications • october 2007.

[7] Mohit Virendra, Shambhu Upadhyaya, Vivek Kumar Vishal Anand ," SAWAN: A Survivable Architecture for Wireless LANs", Third IEEE International Workshop on Information Assurance 2005 IEEE

[8] Vladimir Berman and Biswanath Mukherjee," Data Security in MANETs using Multipath Routing and Directional Transmission", 2006 IEEE.