ISSN:0975-9646

Ashwini Shendre et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5397-5399

Using SG-PKM Improve security mechanism for Supporting Routing Services on WANET

Ashwini Shendre[1]
Department of Computer Science & Engineering
line G.H.R.I.E.T.W., Rashtrasant Tukdoji Maharaj
Nagpur University

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

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.

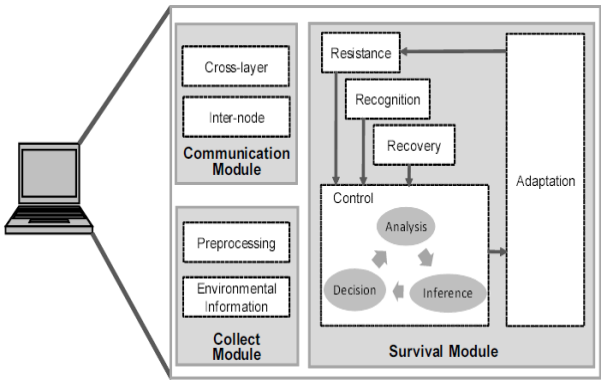


Fig 1. SAMNAR

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.

III. TECHNOLOGIES

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

This is existing architecture .We employe SAMNAR for supporting the development of a survival path selection scheme on routing services. Whose goal is the design of survivable essential network services against attacks and intrusion. The SAMNAR is supported to three defense line preventive ,reactive and tolerance defense line. These three defense line provides some mechanism to work or improve survivability .

Preventive mechanism try to avoids the attack like antivirus .Reactive mechanism detect and react against attack.

Tolerance mechanism giving the solution against damage or failure.

B. *Survival Path selection scheme*

The survival path selection scheme works on a multi criteria based concept .It will select multiple path at a time and giving rank to each path. Providing rank on the basis of time, energy, and distance measure. Those having less time, efficient energy and small distance those paths are selected.

For selecting best path selection scheme here uses the AOMDV(on demand multipath distance vector Routing in Ad-hoc network) protocol is used.

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.

i. *Group certificate* :- Group certificate consist of source and destination group identities ,source and destination node identities ,energy, range, key .

ii. *node certificate*:- node certificate consist of source and destination node identities, energy , range, key

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. figure 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

D. *How to apply certificates on SAMNAR*

The two nodes are transmitting the packets to the each other or communicating with each other .On this transmitting packet also consist of certificate. When best path was discovered it will verify the certificate than it will transmit the packet. When communication is in under process ,if unauthorized person or attacker attack that time it will work. However without verification of certificate the data will not transmit or exchange.

E. Operations of certificate

i. *Create certificate*:- When packate is build certificate also created with packate

ii. *Verification* :- It will verify on the basis of Key exchange through certificate.

iii. *Exchange certificate*:- It will exchange when data transmit

F. Wireless ad hoc networks

Simulation settings: The IEEE 802.11 protocol operating with the distributed coordination function (DCF) is used as medium access control (MAC) protocol.This MAC protocol were use the maximum range is 250. This radio range was used to force a higher number of nodes in multi-hop paths.

The network interface queue size of the nodes was set to 64 packets for routing and data packets. This is a medium access Control (MAC) which work on Distributed Coordinated Function(DCF) . This protocol work on a maximum range i.e 250m .The two nodes can transmit packets or communicate in this range only. It is a radio model for communication with transmission power of 15dbm and received card sensitivity of -93 dbm.

Here uses the IEEE802.11.So the maximum standard range is 250m. This is as per application. If the range increases like 500m then want to use the IEEE802.15 .If range is increase the noise of broadcasting is also increases and also need to increase the power gain and db.

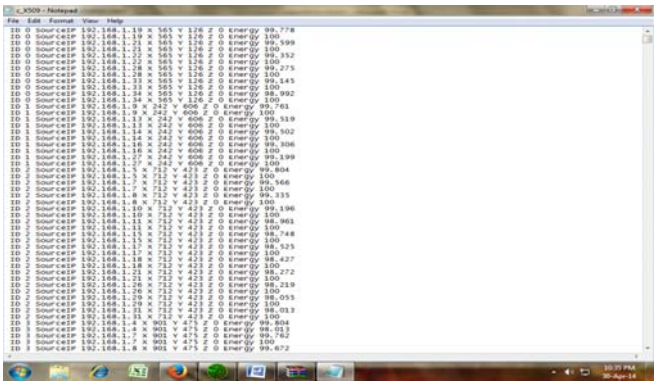
Simulation Result

Our Simulation based project has been designed in VB.Net. Table Shows simulation parameters used in the design.

TABLE . SIMULATION PARAMETERS

Parameter	Description / Value
Routing Protocol	Deluge, SDRP
Nodes	30
Transmission Range	250m
Energy	100J
Mac Layer	802.11

Here uses the certificate concept along with the packate. So certificate also mention with the each packate..The certificate creation is shown below figure.



The simulation results also shown in graphical form, But are in under the processing .So only showing the parameters to show the result in future.

1. Graph shows the dropped packet.
2. Graph for showing percentage of security increases
3. Attack analysis
   In this graph here shows the how this project is work on attack.

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.