Ensure Secure Communication in Ad Hoc Network

GAURAV VISHWAKARMA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

BILASPUR, INDIA

gvishwakarma@gecbsp.ac.in

***Abstract*-- An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. It is a mobile network of new era. In such an environment, it may be necessary for one mobile host to enlist the aid of other host in forwarding a packet to its final destiny, due to the restriction in the (limited area) range of each mobile hosts wireless transmission .the military tactical, highway traffic & other security-sensitive operation are still the main application of ad-hoc network, although there is a trend to adopt ad-hoc networks for commercial uses due to their unique properties .one main challenge in the design of these network is their vulnerability to security attacks. In this paper, we study the threat an ad-hoc network faces and security goals to be achieved. I identify the new challenge posed by this new networking environment & explore new approaches to secure its communication. In this network as we already provide numbers of security features like secrecy, reliability , cryptography etc., but the problem is not only up to this , the main thing is the members in the network are globally authentic or not. If we globally authenticate the user in the network then we can ensure the communication in the network is secure communication.**

***Keywords*-- Globally Substantiation, Secure Communication, Radio Wave Intersection, Packet Broadcast, Ad Hoc Network.**

I. INTRODUCTION

Ad hoc network is a local area network (LAN) that is built spontaneously as device connects. It is a decentralized type of wireless network. It does not rely on pre-existing infrastructure, such as wired network or access point that why it is called ad hoc network. Ad hoc network are a new paradigm of wireless communication for mobile host.in ad hoc network, there is no fixed infrastructure communication. The nodes (mobile device) that are within the radio wave range will automatically detect the network & can communicate directly via wireless links. Minimal configuration and quick deployment make ad hoc network suitable for emergency situation like natural disaster or military conflict.

In an ad hoc network ad hoc is a Latin word means "for this" meaning "for this special purpose" and "extension" also. An ad hoc network proves its meaning true. Figure-1 shows such an example, suppose node A (source) want to send the packet of information to destination node Z which is far away from node A, and the packet of information is very urgent and have to send within the time limit.ad hoc network is very efficient & useful . it will pass packet of information to next node within radio, & like wise to next node, and at last it reached to the destination node Z and if any intermediate node moved out radio range or radio wave intersection area then connection will be lost, but if more than one path is established or we can say that any node is inside the range or intersection area that will make sure the packet of information is delivered.

II. SECURITY MODEL

A. Security

The for most things in any network is security if any network is secure then it is reliable and if not then it is very difficult to use that network. The security attributes that we use in ad hoc network are accessibility, secrecy, reliability, substantiation, and non-repudiation.

B. Reliability

Reliability is particularly important for critical safety and financial data used for activities such as transfers of funds, controlling the air traffics, and financial secretarial. Decisive Information can be erased or become unattainable, resulting in loss of accessibility. This means people who are authorized to get information cannot get required information.

C. Accessibility

Accessibility is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Accessibility of the network itself is imperative to anyone whose business or education relies on a network connection. When a user can't access to the network or precise services provided by the network, they experience a denial of service.

D. Secrecy

It ensures that certain information is never disclosed to illicit entities. Transmission of sensitive information in the network, such as deliberate or tactical information of military, requires privacy. Leakage of such critical information to enemies could have devastating consequences. Steering information must also remain secret in certain cases, because the information might be precious for enemies to spot and to situate their targets in a front line.

E. Attack using fabrication

Generating of false steering message in the wide network is termed as fabrication messages. Such attacks are intricate to spot.

F. Non-repudiation

It ensures that the origin of a message cannot rebuff having sent the message. Non repudiation is useful for revealing and segregation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to sway other nodes that B is compromised.

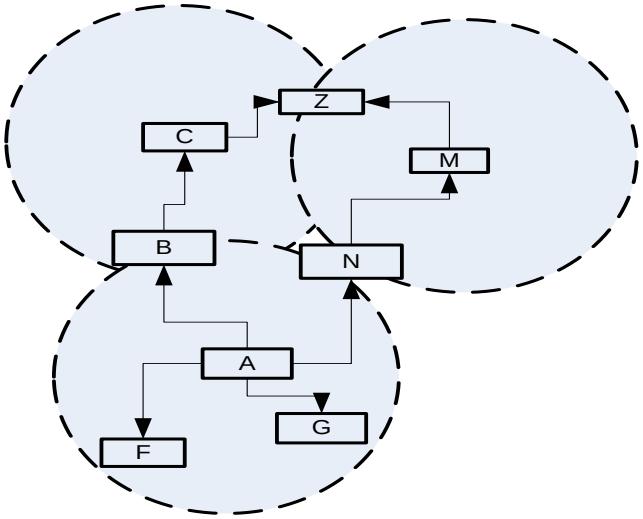

Fig. 1

Node A behave as source node & node Z behave as destination node via intermediate node a transfers the information packet to destination node.

III . RELATED WORK

Recently there have been several papers that have looked for security of ad-hoc network. The security in the sense that communication should be done in between connected nodes,

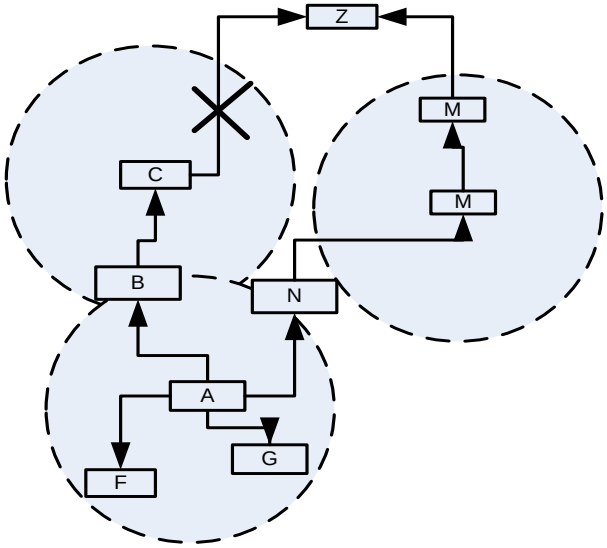

Fig. 2

Information packet from node A to node Z is transfer by multiple path & if any node is moved out from radio range then n/w will disconnect but info-Packet will transfer via different route.

other nodes cannot be able to do so.[12] provides substantiation to the system in order to ensure that the POI is send by the known node. if A is able to identify again the authority that runs B, i.e.is able to convince A that both had some relationship in the past. We also say that A recognizes B, or that B authenticates to A. [16] modified the previously provided protocol by also providing the identification in it. Identification of the node is necessary; if we can't do so then we are unable to verify the system. the key contribution is of both papers is to provide the base of security to the network node one provides the substantiation to the node, and other provides the identification to the network node.

[6] provides the new way to secure the network, it turns thinking of peoples to the new world of security, in this paper we move towards the protocols to route the message earlier we only thinks about the security at the node levels. In this we deals with the protocols, how to make the POI secure in the network, basically this paper secure the network from denial of service attack by establishing a secure key management service in an ad-hoc networking environment. [13] sense the attack on the routing protocol called Dynamic source routing (DSR) protocol and also the originator of the attack, this mechanism to inform other nodes of the system about the accused, provide a perspective aware inference scheme to censure the accused and malicious accuser without doubt. This paper plays a vital role to make the ad hoc network secure, or we can say that this make the ad hoc network more reliable and accessible to wide use, node in the network can send POI without any hesitation.

Till now we only think about or talk about the security till at the node or at route but we not discuss about or verify delivery of quality of service in the network [11] verify the delivery of quality of service in the multi-hop network. In this paper we present protocol that enables Verification of delivered QoS for individual packet as well as verification of statistical QoS for group of packets. The protocols are proved to be cheat proof. This also provides expression for the minimum verifiable delay. The key contribution of this paper is by providing verify delivered QoS in wireless networks.

IV. MODELS AND ASSUMPTION

Before discuss the models lets discuss about the assumption that make for the model is: - (a) n number of nodes are already connected in the ad hoc network. (b) Every node knows that how many nodes are connected with that node or in the link of that

ad hoc network. (c) Suppose any how a new node get into the network by knowing the keys to get connected into the network.

A. GLOBAL SUBSTANTIATION

We employ some techniques of UNIX operating system in our new era network, to make it secure from many attacks. As we all know that the very interesting and important feature of UNIX OS is telnet. Through this features any node of the network can check how many more nodes are connected with us and we can communicate with each other via telnet. One more features of same OS is broadcasting it is also a very crucial & special feature. Now the question arises that how can we use these features in Ad hoc network and why. The simple answer is we employ just similar features in our network to make it more secure. Whenever any new node is entered in our network the parent node will broadcast the POI to all node connected to it and also to its all node in a chain. When this POI is send back by all the nodes with "YES" as reply the only this new node can be able to communicate otherwise he can't be able to access information in the network. This is mainly be much more beneficial for real time operation like army, banks etc.

The technique global substantiation means substantiation is done globally not locally and we also identify the new node whether it is faithful to all existing nodes , when we talk about global substantiation it means all the nodes present in the network authenticate the new node, then, it can be able to join or be the part of the network else it won't be the part of the network since can't be able to communicate in the network. This type of security make levels in of security in the network, when all these level is satisfied by the node then only any node is able to be the part of network otherwise not.

B. HOW MODEL WORKS

The global substantiation is a technique through which we not only authenticate the user but also verify the node is not a member of the enemy network or a node of enemy network or a fraud node, when a new node try to join the network or try to access the network after inserting the password or key to access the node but this technique not employ the new node to directly access the network POI but it directly send a packet containing all the information of the new node to its parent network and then from parent network to all the previously node connected and to the other parent node and their nodes. We don't need to verify the delivery of POI in the multi-hop network this is already done in the previous paper we can directly implement that technique to our network so that it make us more security and reliable.

Suppose in network when new node try to connect and its information is send all existing nodes in the network if all these existing node deny or send "no" as a replay the this new node cannot be able to connect or access the information of the network. The node can only be able to connect to the network when all the existing node send or replay "yes " to the packet, if any single node send replay "no" then new node cannot able to connect.

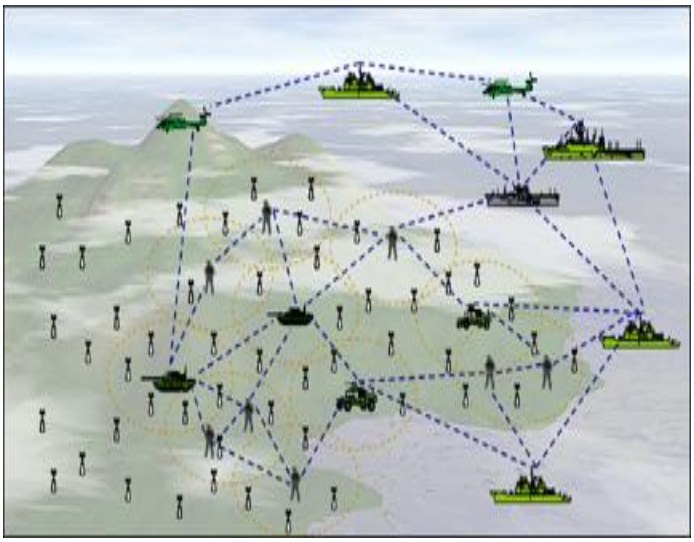

Fig. 3

Suppose army is going to attack on enemy and they form a ad-hoc network to be in contact with each of the node, now if any how enemy get the key of the network of army then he can enter in the network, then the plan of the army disclose to enemy and as a result their plan may fail

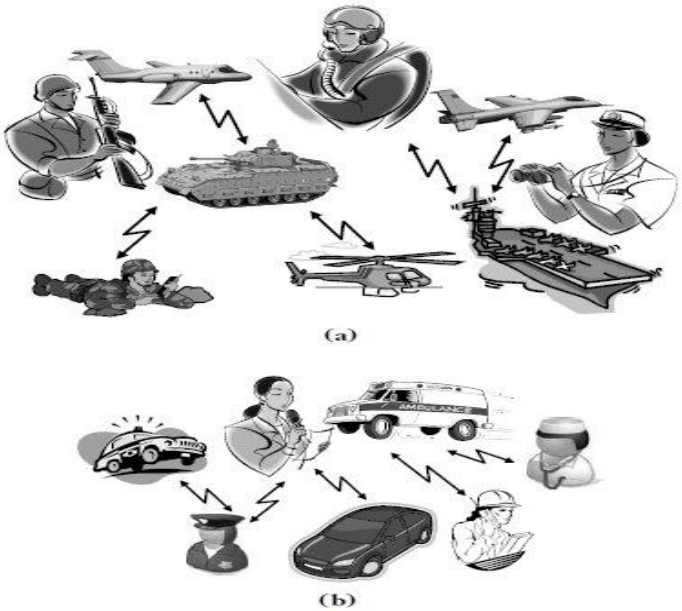

Fig. 4

4. Conclusion

Our technique provides the surety to the network users that after getting the security key by the unauthorized node, but then also he is unable to access the information of the network because until the confirmation from the all the user allow or permit the new node to

join, otherwise he is unable to connect in the network. this make user secure and not to worry about the key of the network.

5. References

[1] Y. Desmedt. Threshold cryptography. European Transactions on Telecommunications, 5(4):449– 457, July–August 1994.

[2] L. Gong. Increasing accessibility and security of an substantiation service. IEEE Journal on Selected Areas in Communications, 11(5):657– 662, June 1993.

[3] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad-hoc wireless networks. Mobile Computing,1996.

[4] C. Kaufman. DASS: Distributed substantiation security service. Request for Comments 1507, September1993.

[5] B. Kumar. Integration of security in network routing protocols. SIGSAC Reviews, 11(2):18– 25, 1993.

[6] Lidong Zhou, Zygmunt J. Haas "Securing Ad-Hoc Networks" Cornell University Ithaca, NY 14853

[7] Katrin Hoeper and Guang Gong "Models of Substantiations in Ad Hoc Networks and Their Related Network Properties" University of Waterloo Waterloo, Ontario, N2L 3G1, Canada

[8] A.O. Salako. Substantiation in Ad hoc Networking, In Proceedings of London Communications Symposium 2002.

[9] C. Perkins. Ad Hoc On Demand Distance Vector (AODV) Routing, Internet Draft, draft-ietf-manet-aodv-00.txt, November 1997, 1997.

[10] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang. Self-Securing Ad Hoc Wireless Networks, Seventh IEEE Symposium on Computers and Communications (ISCC '02), 2002.

[11] Suresh Singh, Tom Shrimpton "Verifying Delivered QoS in Multi-hop Wireless Network" Member IEEE.

[12]Andre Weimerskirch, Dirk Westhoff " Identity certificate substantiation for ad hoc networks" Germany October 31, 2003

[13] Krishna paul, Dirk Westhoff "context aware detection of selfish nodes in DSR based ad hoc network" IEEE GLOBECOM 2002 tiwan November 2002

[14] Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, S. Sajama, Wireless Ad hoc Networks, Wiley-Interscience, December, 2002.

[15] Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, S. Sajama, Wireless Ad Hoc Networks 2002.

[16] André Weimerskirch and Dirk Westhoff, Zero Common-Knowledge Substantiation for Pervasive Networks Tenth Annual Workshop on Selected Areas In Cryptography (SAC '03),14-15 August 2003, Ottawa, Canada