International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, 2020
ISSN: 1475-7192

Security Enhancement in Mobile Adhoc Networks using computational intelligence

[1]T.P.Anithaashri, [2]M.Saravanan

ABSTRACT-- *Mobile Adhoc Networks (MANET) is a collection of wireless nodes that can dynamically form network to exchang**e** information without using any fixed network infrastructure. By using advanced technology in MANET provides the way to serve challenges. MANET are known to be vulnerable to a variety of attacks due to lack of central authority or fixed network infrastructure. In many more security schemes have been proposed to identify misbehaving nodes. In this paper it has been proposed an intelligence based link state routing protocol named ILSR for mobile wireless networks. Thus the protocol is based on the link state algorithm and it is proactive of its nature. It employs occasional exchange of messages to maintain topology information of each network at each node.ILSR is an improvement over a pure link state protocol as it compacts the size of information sent in the messages, and* in *addition, reduces there number of retransmissions to these messages in entire network.. They provide optimal security solution to the current scenario in large and dense ad hoc networks**.***

Keywords--*AODV, ILSR, Routing Protocol attacks, Mobile ad hoc networks.*

I. INTRODUCTION

The human's future living environments are nascent based upon information resource provided by the connections of various communication networks for users. The small devices like Personal digital assistants, mobile phones, handhelds, and wearable computers enhance information processing and accessing capabilities with mobility. In traditional home accessories such as modern camera, cooking machines, washing machines, refrigerators, cleaning equipment with computing and communicating powers attached extend the field to a fully computing environment[7]. With these modern technologies should be formed within the new paradigm of computing including new architectures, tools, protocol, device and services,. Mobile networking is most important technologies during the last ten years, advances in both hardware and software techniques have resulted in mobile hosts and wireless networking common and miscellaneous. Fundamentally there are two distinct approaches for enabling wireless mobile units to communicate with each other.

Infrastructure: Wireless mobile networks have traditionally been based on the cellular concept and to be dependent upon the good infrastructure supports and these mobile devices communicate with access points like base stations connected to the fixed network infrastructures. Representative examples of such kind of wireless networks are GSM, UMTS, WLL, and WLAN. As to infrastructure less approach mobile wireless network is commonly known as a mobile adhoc network (MANET).

[1] Associate Professor, Department of Innovative Informatics, Institute of Computer Science Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, shri3krra@gmail.com, anithaashritp.sse@saveetha.com

[2] Professor, Department of Innovative Informatics, Institute of Computer Science Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, saranenadu@gmail.com,

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

***Infrastructure less*:** A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any preexisting fixed network infrastructure [2,1]. This is important part of communication technology because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on acting configuration of wireless connections on the flown. Wireless adhoc networks are basically independent and wide areas of research and application functions, rather than being only just a complement of the cellular system.

II. RELATED WORKS

Adhoc networking is decade concepts that the technology for dynamic wireless networks, it had been especially in an effective way in military purpose. It is a Latin word and it means for this purpose. This network is a self configure infrastructure less networks of mobile devices and these connected by wireless links [6]. Mobile adhoc networks are self organize nodes, without the need for preexisting infrastructures. Every node in the network acts as a sender and a receiver and as a router at the same times. If the two nodes are in the transmission range of each other then they can communicate directly to this network. Otherwise, they reach each other in the way of multi-hop route. MANET nodes are typically distinction by their processing, limited power and memory resource techniques as well as high degree of mobility. In many networks, the wireless mobile nodes are may progress enter the network as well as leave the network [14].

The Adhoc On-demand Distance Vector (AODV) routing algorithm is a routing protocol designed for adhoc mobile networks. This protocol is capable of both unicast and multicast routing. Its an on demand algorithm meaning that it builds routes between nodes only as longing by source nodes. It standards these routes as long as they are needed by the sources. In extra, AODV forms trees which connect multicast group members. Despite of these trees are composed of the group members and the nodes need to connect members. AODV uses sequence numbers to guarantee the freshness of routes. This is loop free self starting and scale to a large numbers of mobile nodes[12]. The AODV protocol uses route request (RREQ) messages flooded through the network in order to discover the paths required by a source node. An intermediate node that receives a RREQ replies to using a route reply message only has a route to destination, whose corresponding destination sequence number is greater or equal to the one contained in the RREQ[16]. RREQ also contains the most recent sequence number for the destination of which the source node is cognizance. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to the contained in the RREQ functions. If this case, it unicast a RREP back to the source of rebroadcast the RREQ .Nodes keep track of the RREQ's source IP address and broadcast ID. They receive a RREQ message which they have already making processes, they discard the RREQ and do not forward it, once the source node receives the RREP, message may begin to forward data packets to the destination. The source later receives a RREP containing a greater sequence number or contains the same sequence number with small hop count; it may update its routing information for that destination and begin using the better routers. So long as the route remains active, it will continue to be maintained and route is consider as active as long as there are data packets periodically traveling from the source to the destination along that path. While the source stop sending data packet, the links will conventional and eventually be deleted from the intermediate node routing tables [1]. If link breaks occur

when the router is active, if the node upstream of the break propagate route error (RERR) message to the source nodes to inform its unreachable destination.

III. PROPOSED SYSTEM

3.1 Intelligence based Link State Routing (ILSR)

Intelligence based Link State Routing (ILSR) protocol is a proactive routing protocol where the routes are always without delay available when needed. This is an optimization version of a pure link state protocol in which the topological changes cause the overflowing of the topological information to all available hosts in the network. In ILSR protocol continuously maintains routes to all destinations in the network, thus the protocol is beneficial for traffic patterns where a large subset of nodes are communicating with another large subset of nodes, and where the [source, destination] pairs are changing over time. ILSR protocol is well suited for the application which does not allow the long delays in the transmission of the data packets. The best working environment for this ILSR protocol is a dense network, where the most communication is concentrated between a large numbers of nodes. ILSR reduce the control overhead forcing the MPR to propagate the updates of the link states, also the efficiency is gained by the compared to classical link state protocol when the selected MPR set is as small as possible[11,9]. But the negative part of a situation of this is must maintain the routing table for all the possible routes. So there is no difference in small medium networks but when the number of the mobile hosts increases. Then the overhead from the control messages is also increasing. This to control the scalability of the ILSR protocol and besides ILSR protocol work most efficiently in the closely compacted wide networks.

The base stations of a fixed infrastructure networks are directly connected to the core, an AHN is typically connected through a satellite link or a terrestrial switch. This vision requires still some further developments in ad hoc networking. Basic research and potential applications of adhoc networks are evolving together, spurring each other into further achievements. The need for a network application can give the directions for finding the solution to meet the requirements of security issues. The overview of the proposed system is described below:

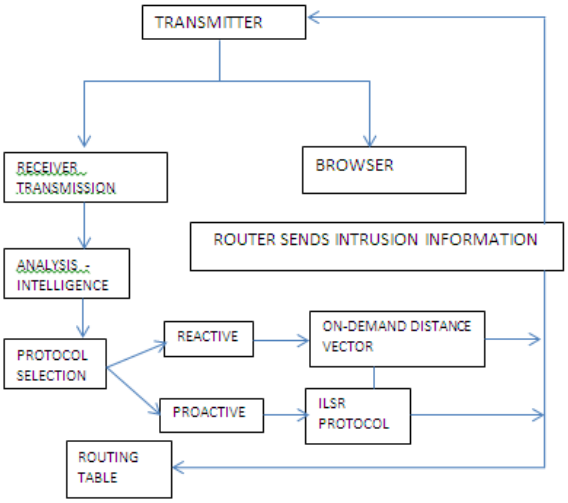

Fig: 1.Overall Architecture of the System

System architecture is the conceptual model that defines the structures, manner and more views of a system. An architecture delineation is a formal of description and representation of a system, arranged according to a system in a way that supports reasoning about the structure of the system which comprises system components, the outwardly visible properties of those components in the relationships between them and provides a plan from which products can be procured, and system developed, that will work together to implement the overall system.

There are basically two approaches to secure MANET, securing adhoc routing and Intrusion Detection. As a preventive measure, the packets are carefully signed but an attacker can simply drop the packet passing through it and they secure routing cannot resist such internal attacks. In our solution provides a reactive scheme that triggers an action to protect the network from future attacks launched by this malicious node. Because of the infrastructure less architecture of our risk-aware response system is distributed and it means each node in this system makes its own response.

In order to evaluate the effectiveness of our adaptive risk aware response solution have divided the simulation process into three stages and compared the network performance. The following describe the activities associated with each stage in providing the security :

Before attack: Random packets were generated and transmitted among nodes without activating any of them as attackers. This module can present the traffic patterns under the normal circumstance.

After attack: Detection or response is not available in this stage. This module can present the traffic patterns under the circumstance with vulnerable activities.

After response: Response decisions for each node were made and carried out based on ILSR protocol.

IV. CONCLUSION

In this paper the adhoc network was introduced and explained how it does differs from the original fixed wired network. The description was given from the adhoc routing protocols and its possible metrics to measure the performance and suitability of adhoc routing protocols were given basing on the RFC paper [17].AODV and ILSR protocols were introduced and their core architecture was described. Due to the basic actions related to the routing process were studied in details and also the advantages of the protocols based on their routing processes were given in the end of the chapters[19]. The comparison was made from the possible protocols advantages and from the literature related to these protocols. The chapter included some results from the papers which compared the following protocols.

Both protocols scalability is restricted due to their proactive or reactive characteristic. In the AODV protocol the flooding overhead in the high mobility networks. ILSR protocol is the size of the routing table and a topological updates messages from scalability of these protocols is quite good and their performances depend a lot from the network environment.

REFERENCES

1. T.P.Anithaashri, G. Ravichandran, R.Baskaran, Software Defined Network Security enhancement using Game Theory, Elsivere COMNET, vol157, pp:112-121, 2019

2. P.Selvi Rajendran,"Virtual Information Kiosk Using Augmented Reality for Easy Shopping",International Journal of Pure and Applied Mathematics (IJPAM). special issue.Volume 118 No. 20 2018, 985-994,Scopus
3. T.P.Anithaashri, G. Ravichandran , et.al. Secure Data Access Through Electronic Devices Using Artificial Intelligence, ICCES, 2018.
4. T.P.Anithaashri, R. Baskaran, Enhancing Multi-user Network using sagacity dismissal of conquered movements, International Journal of American Scientific Publishers pp:69-78, 2016
5. TPAnithaashri and R Baskaran, Reign Monitor service for web enabled distributed system in the International journal on Computation of Power, Energy, Information and Communication,Vol-12 April 2013
6. TPAnithaashri and R Baskaran, Enhancing the Network Security using Lexicographic Ga.me- Second International Conference, Advances in Computer Science and Information Technology-Bangalore, India, Part-III, Jan2-4,2012,.
7. C. Siva Ram Murthy, B.S. Manoj , "Ad hoc Wireless Networks Architectures and Protocols",2011 by Pearson Education Inc., pp. 196.
8. M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network," Ericsson Review, No.4, 2000, pp. 248- 263.
9. Ad Hoc Networking Extended Research Project. OnlineProject. http://triton.cc.gatech.edu/ubicomp/505
10. M.Massey‖The‖ The Attacker in Ubiquitous Computing Environments,‖ unpublished.
11. Todd R.Andel, Alec Yasinsac,‖Adaptive Threat Modeling for Secure Ad Hoc Routing Protocols‖, Electronic Notes in Theoretical Computer Science 197 (2008) 3–14.
12. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing, "Mobile Ad-Hoc Network Working Group,vol. 3561, 2003.
13. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks,"IEEEComm. Magazine,vol. 40, no. 10, pp. 70-75, Oct. 2002.
14. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing,"IEEE Security and Privacy Magazine,vol. 2, no. 3, pp. 28-39, May/June 2004.
15. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A.Jamalipour,"A Survey of Routing Attacks in Mobile Ad Hoc Networks,"IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.
16. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, "Ad Hoc Networks, vol. 1,nos. 2/3, pp. 293-315, 2003.
17. L. Sun, R. Srivastava, and T. Mock, "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory ofBelief Functions,"J. Management Information Systems,vol. 22,no. 4, pp. 109-142, 2006.
18. C. Mu, X. Li, H. Huang, and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08),pp. 35-48, 2008.
19. K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.

20. L. Zadeh, “Review of a Mathematical Theory of Evidence,”AI Magazine,vol. 5, no. 3, p. 81, 1984.[15] R. Yager, “On the Dempster -Shafer Framework and New Combination Rules1,” Information Sciences, vol. 41, no. 2, pp. 93-137, 1987.
21. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, “Sensor Fusion Using Dempster-Shafer Theory,”Proc. IEEE Instrumentation and Measurement Technology Conf.,vol. 1, pp. 7-12, 2002.
22. S. Corson and J. Macker “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations.” RFC 2501, IETF Network Working Group, January 1999.

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020