International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

HYBRID DYNAMIC SECURE ROUTING PROTOCOL FOR REDUCING INTERFERENCE IN MANETS

Dr.S.Soundararajan,
Vice Principal,
Velammal Institute of Technology,
Chennai,India.

R.Swetha Shree,
B.E Student,
Velammal Institute of Technology,
Chennai,India.

T.Anandhi,
B.E Student,
Velammal Institute of Technology,
Chennai,India.

N.Mohanalakshmi,
B.E Student,
Velammal Institute of Technology,
Chennai,India.

Abstract: Jamming-Resilient Secure Neighbor Discovery (JR-SND) scheme which is proposed for MANETs is based on direct-sequence spread spectrum and random spread-code predistribution. Hybrid Dynamic Secure Routing Protocol (HDSR) is used in this mechanism. .JR-SND enables neighboring nodes to securely discover each other with overwhelming probability despite the presence of omnipresent jammers. It considers the battery energy and energy consumption of node as well as quality of links, to find energy-efficient and reliable routes that increase the operational lifetime of the network. HDSR, on the other hand, is an energy-efficient routing algorithm.This algorithm is used to find routes minimizing the total energy required for end-to-end packet traversal. HDSR are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability. In our system, we provide secure transmission using the process of encryption and decryption. In rapidly a day's MANET having many security vulnerabilities, security is very consistent for en masse needs specifically in the orientation of wireless network. JR-SND along with the HDSR protocol is used to identify the jammers between nodes. Because of this jammer communication is not possible. If the jammers are detected and avoided totally, group communication can be done. So to provide one to one communication after the identification of jammers, the receiver's IP address and port number alone is specified. And the transmission is done in a private way. This is done using MANET, in which the trust value model has two components such as trust from direct observation and trust from indirect observation. And with the direct observation from observer node, the trust value is derived using the Bayesian inference method and indirect observation from dempster-shafer theory.

Keywords: Mobile ad hoc networks (MANET), protocol, HDSR, jamming, resilience, jitter

I.INTRODUCTION

An important feature of mobile ad hoc networks (MANETs) is that information can be routed from a source node to a destination node even if the two are not directly connected using a physical link.MANET is a type of ad hoc network that can change location and configure itself.Each device in a MANET is free to move independent.It is continuously self-configuring and infrastructure less network which is used to establish network through collection of mobile nodes.Every node in the network acts as a router which is used to forward the packet to the destination. Information is routed throughother intermediate nodes,in which routes are established in MANETs using one or more routing protocols. One popular MANET routing protocol is Hybrid Dynamic Secure Routing (HDSR). With HDSR, every node proactively maintains routing tables to destination nodes so that information packets can be routed on existing routes, as opposed to establishing routes on-demand.

MANET has many key characteristics such as lac of fixed infrastructure,bandwidth constrained,variable capacity links, dynamic topologies,energy constraints operations, increased vulnerability. Using these key characteristics MANET works on many applications such as communication among portable computers, military, emergency applications. The network topology gets changed randomly due to the mobility of nodes; therefore the security is a major issue in MANETs. Malicious nodes attack the network's availability through common techniques such as flooding, black hole, denial of service. The routing protocol must react to the changes to enable route connectivity. The packet forwarding is done through links for topology based routing protocols. In MANETs there are two types of attacks such as active attack and passive attack. Active attacker tries to break into secured systems.This can be done through worms,trojanhorses.these attacks are against network backbone,transit exploit information it result in disclosure or dissemination of data files or modification of data. MANET is affected by various routing attacksuch as wormhole attacks,blackhole, gray hole,Sybil.We mainly focus on black hole attack which falsely acquires the fresh route to the destination and drops the packet without forwarding. To avoid black hole attacks we use hybrid dynamic secure routing protocol.

II. OVERVIEW OF PROTOCOL JAMMERS

In MANETs, robust routing via intermediate nodes is at the

mercy of the wireless medium. In this section we present a short overview of different types of jammers found in the literature that target wireless signals carrying protocol messages.Wireless signals can be degraded and disabled by jamming techniques where co-channel interference occurs.This interferers disrupt the integrity of the received signal.The High power transmission of the continuous-wave signals within radio range of a target can reduce the signal-to-noise ratio of the target to an unusable level.But this method of jamming also lead the jammer to be detected, located, and removed.As an alternative, a smart jammer only transmit when it senses the channel activity. As an another alternative, a sophisticated smart jammer only transmits when it senses channel activity of the type targeted, e.g., messages of a targeted communication protocol. Such a jammeris also known as protocol jammer. It expends low power and targets messages of specific communication protocols, and as a result, is harder to detect.

III.RELATED WORKS

We present a framework for throughput optimization for multipath unicast routing in wireless networks in the presence of probabilistic jamming. The framework introduces a statistical characterization into the maximum network problem to compensate for the reduction in network due to the loss of jammed packets. We map the problem of throughput optimization under probabilistic jamming to that of optimal investment portfolio selection, treating the network throughput as the return on financial investments and using a common portfolio selection framework from financial statistics. Based on the portfolio selection framework, we present approaches to maximize expected throughput and to minimize throughput variance. We include both a detailed example and a simulation study to illustrate the application of the throughput optimization framework.

Wireless mesh networks (WMNs) contains mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. They give us the network access for mesh and conventional clients. The integrals of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. Mesh clients can either be stationary or mobile, and it form a client mesh network among themselves and with mesh routers. WMNs are anticipated to resolve the limitations and improve the performance of ad hoc networks, wireless local area networks ,Wireless Personal Area Networks (WPANs), and Wireless Metropolitan Area Networks (WMANs). They are undergoing quick progress and inspiring numerous deployments. WMNs will deliver the wireless services for a wide variety of applications in personal, local, campus, and metropolitan areas. Despite recent advances in the wireless mesh networking, many research challenges remain in allthe layers of the protocol. It presents a brief study on recent advances and open research problems in Wireless Mesh Networks. System architectures and applications of WMNs are described, followed by discussing the critical factors influencing protocol design. Theoretical network capacity and protocols for WMNs are explored with an objective to point out a number of open research issues. Typically testbeds, industrial practice, and current standard activities related to WMNs are highlighted.

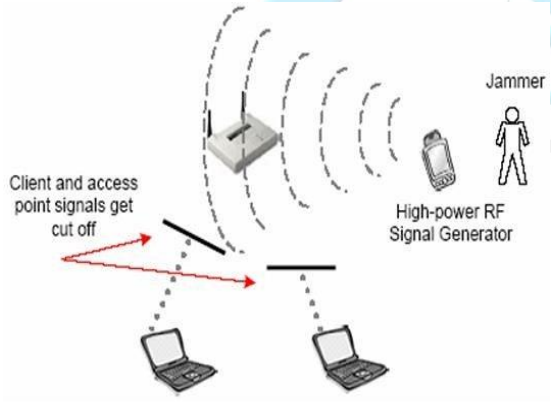
It has long recognized that complete jamming of wireless networks can be realized by generating continuous noise with sufficient power in the vicinity of the wireless network. There are many disadvantages of in this approach such as high energy requirements and a high probability of detection. The purpose is to show that similar jamming effectiveness can be achieved with low energy requirements and low probability of detection. We discuss the variety of measures of performance for jamming and the role of authentication in DoS attacks. Then we can study and simulate, using OPNET 11.5, the effect of periodic jamming on throughput for an MAC network. We can add intelligence to the jammer by using knowledge of the protocol and exploiting critical timings and control the packets. Intelligent jamming is shown to be efficient than continuous jamming in terms of signal duration. The next approach is one that use a node or two to exploit the backoff timer to create a DoS attack. Atlast, we can discuss how these attacks can be applied to the networks with protocols such as MILSTD. Sensor networks promises holding of facilitating large-scale, real-time data processing in complex environments. Their applications will help protect and monitor military, environmental, safety-critical, or domestic facilities and resources. In these and other vital or security-sensitive deployments, keeping the network available for its intended use is essential. The stakes are high: Denial-of-service (DoS) attacks against such networks may permit real-world problem to the health and security of people. Without right security techniques, networks will be confined to be limited, controlled environments, negating much of the promise they hold. The limited ability of individual sensor nodes to prevent failure or attack makes ensuring network availability more difficult. To identify Denial of Service vulnerabilities, we consider two effective sensor network protocols that did not initially consider security. These examples clearly shows that consideration of security at design time is the right way to ensure successful network deployment. In the existing system,OLSR protocol is used.The existing solutions all depend on some publicly known communication strategies such as public spread-code sets. The conflict can use such public knowledge for injecting arbitrary many neighbor discovery requests in the whole network, leading to a special Denial-of-Service (DoS) attack in which all nodes are forced to perform endless verifications of neighbor discovery requests (which often involve expensive digital signature verifications).

IV.PROPOSED APPROACH

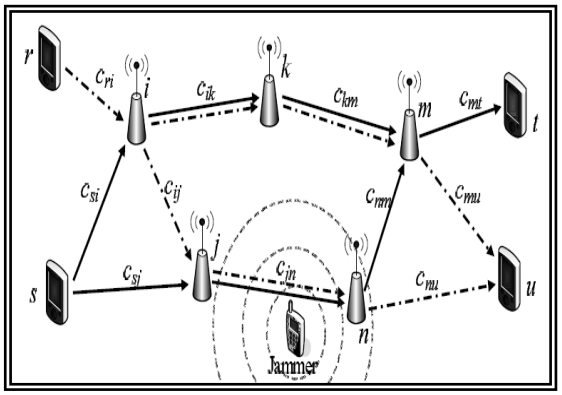
In this,we propose recent advances in trust management scheme that enhances the security in MANET. In the trust management scheme we use hybrid dynamic secure routing protocol

(HDSR) it has two components: Trust value in direct observation and trust value in indirect observation. In direct observation the trust value is derived using Bayesian inference and indirect observation the trust value is derived using dempster- Shafer theory.Indirect observation is also called as second hand information, it is obtained from neighbor node of the observer node. Combining these two components we can get accurate trust value.Theresult show that throughput and packet delivery ratio will be improved and reduce end to end delay and overhead of messages. The proposed algorithm overcomes the problems in the existing optimized link state routing protocol,it acts against the black hole attack and provides a secure and efficient routing in the network.In HDSR protocol,it contain both proactive and reactive protocol.

Multiple-path source routing protocols allows source node to distribute the total traffic among required paths to be travelled . In this article, we consider the problem of jamming-aware among the nodes from which the data is to be transferred.. We show that in multi-source networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM) using HDSR protocol. We demonstrate the network's ability to alculate the impact of jamming and incorporate these estimates into the traffic allocation problem.



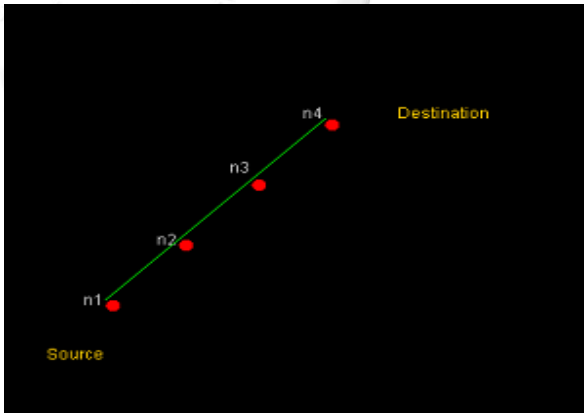
Finally, we do a detection work in order to avoid those jammers and allow a smooth transfer of the datas from one end to the another using the encryption and decryption methods . The below figure shows the transfer of messages from the source to destination and because of the presence of jammer data is being transmitted in some other path.process, we speak of multipath routing. Mobile ad hoc networks (MANETs) are characterized by the dynamic topology, limited channel bandwidth and limited power at the nodes. Because of these characteristics,the paths connecting the source nodes with destinations may be very unstable and go down at any time, making communication over ad hoc networks difficult. On the other hand, as all nodes in an ad hoc network can be connected dynamically in an arbitrary manner, it is normally possible to establish more than one path between a source and a destination ,when this property of ad hoc networks is used in the routing.



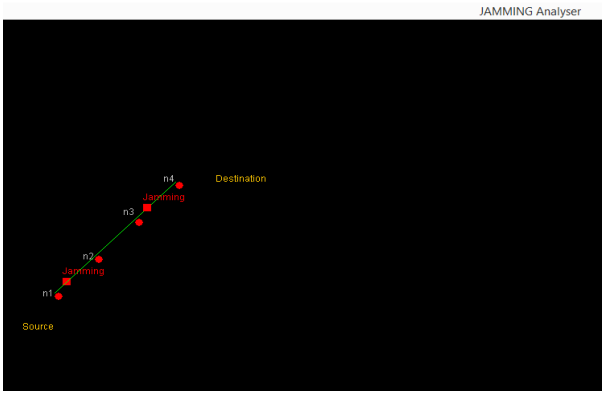
Jamming point-to-point transmission in a wireless mesh network or underwater acoustic network can have delaying the effects on data transport through the network. The effects of jamming at the physical layer resonates through the protocol stacks, providing an effective DoS (denial-of-service) attack on end-to-end data communication. The simplest methods to guard a network against jamming attacks comprise physical layer solutions such as spread-spectrum or beam forming, which forces the jammer to expend a greater resource to reach the same goal. However,the recent work has demonstrated that the intelligent jammers can incorporate cross layer protocol informations into jamming attacks**.**

V .RESULTS

BEFORE JAMMING



The nodes are initially in their respective positions. Here we assign only four nodes and the transfer of the files from one node to another node is checked.The files are splitted based on the file capacity.The files are then encrypted using RSA algorithm and the files are decrypted on the receiver side .We detect for the presence of the jammer.If the jammer occurs the file should be resend.



AFTER JAMMING

VI. CONCLUSION

The security of the MANETs are enhanced via trust management using direct and indirect observation evaluating the trust values for the observed dropping nodes. The modified packets can also be detected. By using the HDSR algorithm ,it helps us to find and improve the attackers detection accuracy and also improves the performance of the network. By using HDSR end to end delay is minimized. Our future work involve enhancing our projects to MANETs in cognitive radios.

REFERENCES

[1]Multipath Rate based Congestion Control for Mobile Ad Hoc NetworksSoundararajan, S.andR.S. Bhuvaneswaran Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, India Ramanujan Computing Center, College of Engineering, Guindy, Anna University, Chennai, India

[2] Multipath Load Balancing &RateBased Congestion Controlfor Mobile Ad Hoc Networks(MANET)Soundararajan**, S.** and R.S. BhuvaneswaranDepartment of Computer Science and Engineering,Velammal Institute of Technology, Chennai, IndiaRamanujan Computing Center, College of Engineering, Guindy, Anna University, Chennai, India

[3]Throughput Optimization for Multipath Unicast Routing Under Probabilistic Jamming: Patrick Tague, SidharthNabar, James A. Ritcey, David Slater, and RadhaPoovendran IEEE 2008.

[4]Wireless mesh networks: a survey Ian F. Akyildiz a, Xudong Wang b,*, Weilin Wang ba Broadband and Wireless Networking (BWN) Lab, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA b Kiyon, Inc., 4225 Executive Square, Suite 290, La Jolla, CA 92037, USA.

[5]Underwater acoustic networks:EMSozer, M Stojanovic… - IEEE journal of oceanic …, 2000 - ieeexplore.ieee.org

[6]Intelligent jamming in wireless networks with applications to 802.11b and other networks: David J. Thuente and MithunAcharyaIEEE 2006

[7]Denial of service in sensor networks:AD Wood, JA Stankovic - computer, 2002 - ieeexplore.ieee.org

[5]Xu, W., Ma, K., Trappe, W. and Zhang, Y., Jamming sensor networks: attack and defense strategies. Network, IEEE, 2006.20(3): p. 41-47.

[8]Xu, W., Trappe, W., Zhang, Y. and Wood, T., The feasibility of launching and detecting jamming attacks in wireless networks, in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing2005, ACM: Urbana-Champaign, IL, USA. p. 46-57.

[9]Thuente, D. and Acharya, M. Intelligent jamming in wireless networks with applications to 802.11b and other networks. in IEEE MILCOM. 2006.

[10]Bicakci, K. and Tavli, B., Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. Comput. Stand. Interfaces, 2009.31(5): p. 931-941.
Wireshark(TM). www.wireshark.org.

[11]TP-Link.http://www.tp-link.com/en/products/details/TL-WN722N.html.

[12]Lin, S. and Costello, D.J., Error Control Coding, Second Edition. 2004: Pearson Prentice Hall.

[13]Salmanian, M. and Li, M. Enabling Secure and Reliable Policy-based Routing in MANETs. in IEEE MILCOM. 2012.

[14]Salmanian, M., Brown, J.D., Li, M. and Mason, P.C.A Covert System Monitoring Function.in NATO Information Systems Technology Panel

[15]Symposium, Information Assurance and Cyber Defence (IST-111/RSY-026). 2012.