www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-4, Issue-6, Dec 2016
Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Investigation for Protection against Jamming attacks and Routing Improvement through Taguchi's loss function in MANET

P. Chouksey

Dept. of CSE, Technocrats Institute of Technology, RGT University, Bhopal, India

Received 24th Sep 2016, Revised 10th Oct 2016, Accepted 23rd Oct 2016, Online 30th Dec 2016

Abstract— Mobile ad-hoc communication is a type of wireless network which is a communications less and decentralized management network. To give secluded communication between mobile nodes the security becomes significant issue in mobile ad-hoc network. Having unique characteristic of MANETs, number of important challenge are there for security design. In this paper we examine number of protection mechanism beside jamming attack and get better quality of network service with the help of Taguchi loss function computation based. In this study paper, we identify a variety of jammer attacks, security goal and existing prevention mechanism after that we proposed taguchi's loss function base node drop identification and neighbor faith measurement base security measurement that proposed technique is better idea for communication performance improvement under security continued existence condition.

.

Keywords— MANET, Taguchi loss function, AHV, RTS, CTS, OTCL

I. INTRODUCTION

A mobile ad hoc network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and examine detection with no the help of an established infrastructure. Decisions may be taken by its own in the mobile ad hoc network. Taguchi's loss function is use to optimize the multiple metrics at the same time in the ad-hoc networks. To protect both route and data forwarding operations in the network any reliable solution for security is necessary Taguchi's loss function finds the reason of presentation squalor in MANET. Nodes of an ad hoc network rely on one another in forwarding a packet to its end, due to the limited range of each mobile host's wireless transmissions. Security in MANET is an necessary component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Unlike networks using devoted nodes to hold up basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are approved out by all available nodes [1]. This very dissimilarity is at the core of the safety problems that are specific to ad hoc networks. As opposed to devoted nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions.

MANET can be established very gymnastically without any fixed base station in battlefield, military applications, and other crisis and disaster situation. Some applications of MANET technology could include industrial and commercial applications involving helpful mobile data exchange. Taguchi's loss function is use to optimize the multiple metrics at the same time in the ad-hoc networks.

The association of weights in multiple performance metrics problems is a critical stage in the whole decision making process [5]. There is no one standard method in determining a metric weight although many methods have been developed as Diakoulaki et all discussed which include assigning weight based on standard deviation, correlation matrix and method CRITIC. In this work, weight based on correlation matrix is used. Weight based on standard deviation has been discussed in [4].

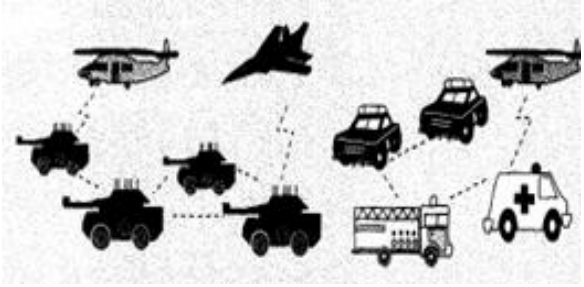

Figure 1 Example Applications of MANET

II. LITERATURE SURVEY

In the wireless communication, jamming is believe as DOS attack, which disrupt the usual working of physical or link layers in lawful nodes by transfer unlawful signals. Jamming is one of such ease of use attacks which can be

easily carried out. It is defined as the future transmission of radio signals that disturb lawful communication by decreasing signal to noise ratio. The author in [2], define the usual jamming & suggest taxonomy of jamming attacks & counter actions in wireless networks. The author in [3], define the jamming attack in MANET & also give the detection method by the measurement of error distribution. The author in [4], introduce switched beam directional antennas in wireless sensor network.

2.1 Jamming Attack Models

Jammer can do a variety of dissimilar attack strategy in order to get in the way with other wireless communication. As occurrence of their dissimilar attack, the diversity of attack models will have dissimilar levels of effectiveness, and may also need different discovery plan. Some possible strategies are expressed below [5]:

- **Constant Jammer:** Stable jammer constantly send out random bits to the channel with no following any MAC-layer manners. Specifically, the constant jammer does not wait for the canal to become inactive previous to transmitting. If the underlying MAC protocol determine whether a channel is idle or not by comparing the signal strength measurement with a set doorstep, which is more often than not lower than the signal strength generated by the constant jammer, a constant jammer can efficiently stop legitimate traffic source from attainment hold of channel and sending packets.
- **Random Jammer:** Instead of incessantly sending out a radio signal, a random jammer alternate between sleeping and jamming the channel. In the first mode the jammer jam for a random period of time, and in the second mode (sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.

2.2 Reactive Jammer: In the reactive jammer, it is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. We would like to point out that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. The primary advantage for a reactive jammer, however, is that it may be harder to detect.

2.3 Security Goals

Security is considered an essential factor in the mobile ad hoc network. In MANET, all networking responsibilities like routing and forwarding the packets, are done by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

- **Availability**: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.
- **Confidentiality**: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.
- **Integrity**: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.
- **Authentication**: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.
- **Non repudiation**: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.
- **Anonymity**: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.
- **Authorization**: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

2.4 Taguchi's Loss Function

Taguchi's loss function parameter design is a powerful technique to determine the optimal combination parameters. The main objective is to use Taguchi design for predicting the better parameters that can optimize the performance metric through the setting of design parameters and reduce the sensitivity of the system performance to the source of variation [6].

The OAs allows researchers or designers to study many parameters simultaneously and can be used to estimate the effects of each parameter independent of the other parameters. Taguchi used a loss function to calculate the deviation between the experimental value and the desired value. The loss function is different for different objective functions. Typically, higher throughput and lower the number of packet drop and routing overhead are desire able

in ad-hoc networks system. Therefore, to obtain optimal ad-hoc network design, the larger-the-better performance metric for throughput must be taken.

III. RELATED WORK

In this section we discuss about the previous work that has done in the field of proposed research title.

Hossen Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu and Adrian Perrig in this work [7] examined multipath routing protocols that will react to communication disturbance on-demand. In particular, a source node selects multiple different paths for reaching the destination in advance. The availability histories of paths are efficiently recorded and calculated via "availability history vectors". Leveraging AHVs, we have presented two AHV-based multipath selection algorithms: one selects multiple paths with the full knowledge of AHVs in the network, and the other computes the path in a distributed manner. AHV-based algorithms can effectively identify multiple paths that provide high end-to-end availability, even in the presence of a new jammer that did not affect the network before path selection.

Kwangsung Ju and Kwangsue Chung [8] "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks" In this tile, in order to overcome limitations of the previous research, we propose a new robust rate adaptation scheme that is resilient to jamming attack in a wireless multi-hop tactical network. Through the performance evaluations, we prove rate adaptation scheme that improves packet delivery ratio and the wireless link utilization.

Mr. Vinod Mahor, Sandeep Raghuwanshi in this work [9] presents the application of Taguchi's loss function approach, a multi-response optimization method, for achieving better performance during routing process of ad-hoc on demand distance vector (AODV) routing protocol. Seven parameters namely terrain size, network size, number of sources, transmitted packet rates, pause-time, node speed, and transmission range are optimized with considerations of multiple performance metrics including maximum packet delivery ratio and minimum routing overhead, packet drop and end-to-end delay. Based on multiple signal-tonoise ratio (MNSR), optimum levels of parameters have been identified and significant contribution of parameters is determined by analysis of variance (ANOVA).

Geethapriya Thamilarasu, Sumita Mishraand Ramalingam Sridhar [10] "Improving Reliability of Jamming Attack Detection in Ad hoc Networks" In this work, we focus on jamming type DoS attacks at the physical and MAC layers in 802.11 based ad hoc networks. Collisions in wireless networks occur due to varying factors such as jamming attacks, hidden terminal interferences and network congestion. We present a probabilistic analysis to show that collision occurrence alone cannot be used to conclusively determine jamming attacks in wireless channel. To increase the reliability of attack detection, it is necessary to provide enhanced detection mechanisms that can determine the actual cause of channel collisions. To address this, we first investigate the problem of diagnosing the presence of jamming in ad hoc networks. We then evaluate the detection mechanism using cross-layer information obtained from physical and link layers to differentiate between jamming and congested network scenarios. By correlating the cross-layer data with collision detection metrics, we can distinguish attack scenarios from the impact of traffic load on network behavior. Through simulation results we demonstrate the effectiveness of our scheme in detecting jamming with improved precision.

Arif Sari and Dr. Beran Necat [11] "Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism" in this title we discuss applied for preventing and mitigating jamming attacks is implemented at the MAC layer that consist of a combination of different coordination mechanisms. These are a combination of Point Controller Functions (PCF) that are used to coordinate entire network activities at the MAC layer and RTS/CTS (Clear-To-Send) mechanisms which is a handshaking process that minimizes the occurrence of collisions on the wireless network. The entire network performance and mechanism is simulated through OPNET simulation application.

G.S. Mamatha, Dr. S.C. Sharma, [12] "Network Layer Attacks and Defence Mechanisms in MANETS- a Survey" In this title a study that will through light on such attacks in MANETS is presented. The title also focuses on different security aspects of network layer and discusses the effect of the attacks in detail through a survey of approaches used for security purpose.

Rajeev kumar, Anshuman kr. Saurabh [13] "A Review on mobile Ad-hoc Network and attacks Happened at Different Layers" The main focus in this title is on attacks security measures at different layers in MANET. Which prevent attacks and attack happen in MANET because security is the most dominating factor.

CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma [14] "Security Challenges and Attacks in Mobile Ad Hoc Networks" This title provides a comprehensive study of attacks against mobile ad hoc networks. We present a detailed classification of the attacks against MANETs.

K. Sivakumar, dr. G. Selvaraj, [15] "Overview of Various Attacks in Manet and Countermeasures for Attacks" In this title, we analyze the security problems in MANET and present a few promising research directions. On the prevention side, various key and trust management schemes have been developed to prevent external attacks from outsiders, and various secure MANET routing protocols have been proposed to prevent internal attacks

originated from within the MANET system. On the intrusion detection side, a new intrusion detection framework has been studied especially for MANET. Both prevention and detection methods will work together to address the security concerns in MANET.

IV. PROPOSED METHOD

In this work we will made an important observation that no measurement is sufficient to reliably classify jamming attack. We build our work on the basis of this observation and develop a detection and prevention mechanism that removes the ambiguity in detecting jamming from congested scenarios. In this work, we will focus on detecting jamming attacks that occur at both MAC layers and network layer of an 802.11 ad hoc network. We present a distributed monitoring mechanism to choose monitor nodes responsible for identifying channel accessibility. The proposed security scheme is able to handle the jamming attack conditions and resolve the problem of link blockage from jamming. Taguchi's loss function is finding the factors that degrades the network performance like network size, nodes etc. These factors are degrades the performance due to random deployment of mobile nodes in large area or very small area but if we covers these parameters through changing in different factors which is suitable and in favor of network condition it implies that the network performance is improves at that conditions then Taguchi's loss function is very important. The implementation strategy of proposed work is mentioned below.

Security is an essential requirement in MANET. Without any proper security solution, the malicious node in the network will act as a normal node which causes heavy flooding of control packets and this flooding is start to a few number of packets and after some time the massive number of packets are flooded in network generally known as jamming attack. In this research we will proposed the security scheme against jamming occurred in the in MANET. Jamming attack is one of the attacks in MAC layer in terms of channel access, bandwidth allocation and in network layer in terms of packets. This attack is comes under security active attacks in MANET. The Taguchi's loss function is measured that which factor (like mobility, network area, number of nodes etc.) is affected the performance of network after applying security scheme.

SAMPLING DESIGN

Jamming attack can be done locally and remotely, and it is one of the most common types of security attacks, because it requires only regular and inexpensive resources, and does not require high technical knowledge. The flooding packets and sophistication of packets are rapidly increasing based on several techniques including direct active attacks. Such security threat that prevents authorized users from gaining access to the wireless channel by disrupting network operations, impacting network connectivity and availability. The main problem in network is that there are many factors like nodes mobility, number of nodes and transmission range are also affected the performance of network and due to which reason the performance is degraded too much is not evaluated individual. The security scheme is protect the network from attacker but if to resolve the degradation from other factor is the major problem issue in MANET.

Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. Taguchi's loss function able to measured the factor that degrades the network performance. The proposed scheme will definitely improves the network performance i.e. measured through performance metrics and provides the zero percentage infection after applying the security scheme against jamming attack. Taguchi's loss function is applied after security scheme against jamming attack and the network performances is measured in different network factor and improve that factor in secure network.

DATA COLLECTION STRATEGY (PRIMARY & SECONDARY METHODS)

For data collection and implementation we will use Network Simulator- 2 (NS-2). The description about simulation environment is as follows:

Network simulator 2 (NS2) is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [16]. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multipath protocol.

The simulator is written in C++ and a script language called OTcl. Ns use an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called Network Animator.

Step 1 – Create network by Ns-2 in TCL.

Step 2 – Insert a jamming node to create a jamming problem

Step 3 – Identify reason for packet drop and apply AHV algorithm for jamming detection.

Step 4 –

Case 1 – (a) Apply proposed security scheme in which three cases are going to consider. In first case after detecting jamming find a new path for transmission, in second case block jamming node and in third case send message to sender to send packets slowly.

(b) Attacker infection is zero then network is secure.
(c) AOMDV use for provide attacker free path for provides better routing performance.
Case 2 – If data is dropped due to different factors then apply taguchi's loss function and evaluate the factor that degrades maximum performance.
Step 5 – Block attacker activities and provide secure environment.
The interpreted class hierarchy is automatically established through methods defined in the class Tcl Class. user instantiated objects are mirrored through methods defined in the class Tcl Object. There are other hierarchies in the C++ code and OTcl scripts; these other hierarchies are not mirrored in the manner of Tcl Object. In order to setup the simulation network in ns2, you must use a language called Tcl. It actually uses an extension of Tcl, called OTcl, which incorporates objects into Tcl. access an interactive OTcl prompt by running the ns command (from a Linux shell or Cygwin on Windows, for example).

SIMULATION STRATEGY

NAM is a very good visualization tool that visualizes the packets as they propagate through the network.

V. PLANNING OF ANALYSIS OF DATA

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc.

According to below table 1 we simulate our network.

Table 1: Simulation parameter

Number of nodes	50
Simulation area	800×600
Propagation of signals	Two Ray Ground
Routing Protocol	AOMDV
Work on Attack	Jamming Attack
Simulation time (sec.)	100
Transport Layer	TCP ,UDP
Traffic type	CBR , FTP
Packet size (bytes)	1000
Traffic connections	10
Maximum Speed (m/s)	30 /s

Performance Measure

The following performance matrices are used to measure the performance against jamming attack and measure the performance factors through Taguchi's loss function that improves network performance.

- **Packet Delivery Ratio:** The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.
- **Average End-to-end Delay**: This includes all the possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.
- **Packet Dropped:** The routers might fail to deliver or drop some packets or data if they arrive when their buffer are already full. Some, none, or all the packets or data might be dropped, depending on the state of the network, and it is impossible to determine what will happen in advance.
- **Routing Load:** The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet or each hop counts.

5.2 Practical Approach

For deployment of secure wireless ad-hoc network the mobile devices are used which support MANET routing capability for that purpose we use Android based devices and inbuilt our module into android based phone and prevent the MANET as well as improve the quality of service of the network, but know a day MANET feasible devices not available in the market.

5.3 Application for Society

Mobile ad-hoc network in recent-trends not available where it is fully deployed so that provide free communication network and that cut the cost of service provider, easily any where public communicate without the need of infrastructure, that helps emergencies situation where infrastructure not exist.

VI. CONCLUSION AND FUTURE WORK

MANETs provide a possibility of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate via access points (fixed structures). Each mobile node acts as a host when requesting or providing information from or to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network.

Taguchi's loss function able to measured the factor that degrades the network performance.

The future simulation of proposed scheme will definitely improves the network performance i.e. measured through performance metrics and provides the zero percentage infection after applying the security scheme against jamming attack. Taguchi's loss function is applied after security scheme against jamming attack and the network performances is measured in different network factor and improve that factor in secure network.

REFERENCE

[1] Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee ,Aniruddha Bhattacharyya ,Arnab Banerjee , Dipayan Bose, "*Study Of Different Attacks In Manet With Its Detection & Mitigation Schemes*" International Journal of Advanced Engineering Technology IJAET/Vol.III/ Issue I/January-March, 2012/383-388.

[2] Yu-seung Kim, Heejo Lee., "*On classifying and evaluating the effect of jamming attack*",

[3] Ali Hamieh, Jalel Ben-Othman., "*Detection of jamming attacks in wireless ad hoc networks using error distribution*." p.p.1-6,IEEE 2009.

[4] John Dunlop and Joan Cortes. "*Impact of Directional Antennas in Wireless Sensor Networks.*", pp.1-6, IEEE 2007.

[5] Wenyuan Xu, Wade Trappe,Yanyong Zhang and Timothy Wood., "*The feasibility of launching and detecting jamming attacks in wireless networks.*"

[6] R.K. Roy, Design of Experiment Using Taguchi, "*Approach: 16 Step to Product and Process Improvement*", John Wiley & Sons, Inc., Toronto,pp. 211- 214, 2001.

[7] Hossen Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu and Adrian Perrig, "*Jamming-Resilient Multipath Routing", IEEE Transactions on Dependable And Secure Computing*," Vol. 9, No. 6, pp. 852-863, November/December 2012.

[8] Kwangsung Ju and Kwangsue Chung "*Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks*" International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

[9] Mr. Vinod Mahor, Sandeep Raghuwanshi, "*Taguchi's Loss Function Based Measurement of Mobile Ad-Hoc Network Parameters under AODV Routing Protocol*", IEEE 4th ICCCNT 2013,July 4-6, 2013, Tiruchengode, India.

[10] Geethapriya Thamilarasu, Sumita Mishraand Ramalingam Sridhar "*Improving Reliability of Jamming Attack Detection in Ad hoc Networks*" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[11] Arif Sari and Dr. Beran Necat "*Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism*" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012.

[12] G.S. Mamatha, Dr. S.C. Sharma, "*Network Layer Attacks and Defence Mechanisms in MANETS- A Survey*" International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010.

[13] Rajeev Kumar, Anshuman Kr. Saurabh, "*A Review on mobile Ad-hoc Network and attacks Happened at Different Layers*", International Conference on Recent Trends in Engineering & Technology (ICRTET2012) ISBN: 978-81-925922-0-6.

[14] CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma "*Security Challenges and Attacks in Mobile Ad Hoc Networks*" I.J. Information Engineering and Electronic Business, 2013, 3, 49-58 Published Online September 2013.

[15] K. SIVAKUMAR, Dr. G. SELVARAJ, "*Overview of Various Attacks in Manet and Countermeasures for Attacks*" International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013.

