RESEARCH REVIEW JOURNALS
Volume-04
Issue-04
April -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Input Investigation for Protection against Jamming Attacks and Routing Improvement through Taguchi's Loss Function in MANET

[1]Sonika Thapak & [2]Dr. Pradeep Chouksey

[1]*Research Scholar, Department of Computer Science, Mewar University, Rajasthan (India)*
[2]*Department of Computer Science, TIT Bhopal, Mewar University, Rajasthan (India)*

ARTICLE DETAILS
Article History
Published Online: 15 April 2019

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

ABSTRACT
Mobile ad hoc communication is a type of wireless network that has decentralized management and no infrastructure. Protection is a vital necessity in mobile ad hoc system to offer secured communication between mobile nodes. Because of specific characteristic of MANETs, it makes a selection of consequential issues to its protection design. In this particular paper we investigate number of defense mechanism against jamming attack as well as enhance the quality of community program by using Taguchi loss function calculation based. In this particular research paper we recognize several jammer attacks, current prevention and security end goal mechanism after we proposed taguchi's loss function base node drop identification & neighbour trust measurement base security measurement that proposed strategy is much better idea for communication performance improvement under security survival condition.

1. Introduction

From A mobile ad hoc network (MANET) involves a pair of mobile hosts who handle fundamental networking capabilities as packet forwarding, routing, and also service discovery without the assistance of a recognized infrastructure. It's the tendency to take choices on its own that's autonomous state. Taguchi's loss function is use to enhance the many metrics concurrently in the ad hoc networks. An integrated security solution is a lot needed for networks to safeguard each information and also route forwarding businesses within the system. Taguchi's loss function discovers the main reason of performance degradation in MANET. Nodes of an ad hoc system depend on each other in forwarding a packet to the desired destination of its, on account of the restricted selection of every mobile host's wireless transmissions. Security in MANET is a crucial part for basic network operates as packet forwarding and also routing: network operation can be jeopardized whether countermeasures aren't embedded into basic network operates in the first stages of the design of theirs. Unlike networks applying dedicated nodes to allow for simple features as packet forwarding, routing, and also community management, in ad hoc networks those capabilities are completed by all usual nodes [one]. This extremely difference is in the center of the security conditions which are particular to ad hoc networks. As opposed to dedicated nodes associated with a classical network, the nodes of an ad hoc network can't be reliable for the appropriate execution of critical community functions.

MANET is usually proven very flexibly without a fixed base station in battlefields, disaster situation, additional crisis along with and also military uses. A number of uses of MANET technological innovation can include commercial and industrial uses involving cooperative mobile information exchange. Taguchi's loss function is use to enhance the many metrics concurrently in the ad hoc networks. With the assistance of taguchi's loss function we calculate loss function which is denoted as L_{ij}

$$L_{ij} = \frac{1}{r}\sum_{k=1}^{n}\frac{1}{y2ijk} \quad (1)$$

Where *r* is the number of repetitions for each trial and *yijk* is the experimental value of the *i*th performance metric in the *j*th trial at the *k*th repetition.

The loss function *Lij* for the smaller-the better performance metric can be expressed as

$$L_{ij} = \frac{1}{r}\sum_{k=1}^{n} y2ijk \quad (2)$$

The Quality of service of the network measure with the help of that equation

The normalized loss function can be computed using [3]:

$$Nij = \frac{Lij}{L*} \quad (3)$$

Where *Nij* is the normalized loss function of the *i*th metric in the *j*th experimental run and *Li** is the maximum loss function of the *i*th metric due to *n* trial. Values of *Nij* are ranging from zero to one. For computing the total normalized loss function corresponding to each trial condition, a weighting factor for each metric considered should be assigned. The total loss function *TLij* in the *j*th trial is defined as

$$TL_j = \sum W_i N_{ij} \quad (4)$$

Where wi is the weighting factor for ith metric and m is the number of metrics under study. The purpose of weighting element is expressing the value of each metric distant relative to other metrics. The association of weights in several performance metrics issues is a crucial phase in the entire decision making process [five]. There's nobody common technique in figuring out a metric weight although many strategies are already created as Diakoulaki et most discussed including setting fat based on standard deviation, correlation matrix plus method CRITIC. In this work, fat based on correlation matrix is used. Fat based on standard deviation was reviewed in [4].

Assuming there are k metrics, weight for jth metrics is formulated as follows:

$$Wj = = Rj / \sum_{j=1}^{k} Rj$$
$$And_{rj} = \sum |Ril| \quad j = 1 \ldots \ldots k, l = 1 \ldots \ldots k \qquad (5)$$

Where *r*jl is the correlation coefficient between *j*th and *l*th metric that measures the degree of the relationship between metric j and metric l and the sum of weight from each metric should be equal to one .[3]

After the values of total loss function are obtained, then it is further transformed into a multiple signal-to-noise ratio (MSNR).

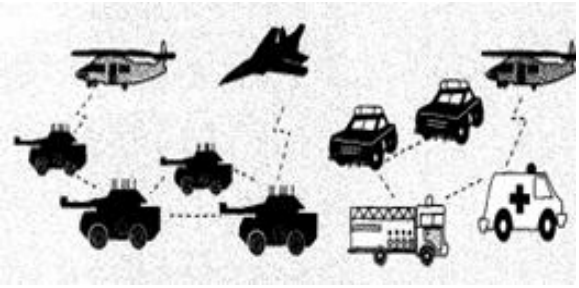

Figure 1 Example Applications of MANET

2. Literature Survey

In order to place Jamming is but one kind of denial of service attacks in the wireless communication, and that disturbs the functioning of physical or maybe link levels in genuine nodes by transferring illegitimate signals. Jamming is one of that "availability attacks which is usually quickly carried out. It's described as the planned transmission of radio signals which interrupt genuine reception by minimizing signal to noise ratio. The writer in [2], determine the standard jamming & propose taxonomies of jamming countermeasures and attacks in wireless networks. The writer in [3], determine the jamming episode of MANET & offer the detection technique by the measurement of errors division. The writer in [4], introduced switched beam directional antennas in wireless sensor system.

2.1 Jamming Attack Models

Jammer is able to do a variety of different hit techniques to be able to hinder other wireless communication.As a trend of the different attack philosophies of theirs, these different episode models are going to have unique levels of effectiveness, and also might also need various detection methods. A few possible techniques are conveyed below [5]:

- **Constant Jammer:** Constant jammer constantly sends out random bits on the channel without adhering to some MAC layer etiquette. Particularly, the continual jammer doesn't hang on for the channel to be nonproductive prior to transmitting. Whenever the basic MAC protocol determines if a channel is nonproductive or perhaps not by looking at the signal strength measurement with a fixed threshold, and that is generally smaller compared to the signal strength produced by the continual jammer, a continuous jammer may efficiently avoid genuine traffic resources from getting hold of channel & driving packets.
- **Deceptive Jammer:** it's distinct from continues jammers. Rather than sending out arbitrary bits, the misleading jammer continually injects frequent packets to the channel with no gap between consequent package transmissions.
- **Random Jammer:** Rather than constantly mailing away a radio signal, a random jammer alternates between sleeping as well as jamming the channel. Within the very first method the jammer jams for a random period of time, and in the next method (sleeping mode) the jammer converts the transmitters of its off for another arbitrary time. The power efficiency is set when the ratio of the duration of the jamming time period with the length of the sleeping time.
- **Reactive Jammer:** In the reactive jammer, it's not essential to jam the channel when no one is talking. Rather, the jammer remains hushed if the channel is idle, but begins transmitting a radio signal the moment it senses exercise on the channel. As an outcome, a reactive jammer focuses on the reception of any message. We'd love to mention that a reactive jammer doesn't always save electricity because the jammer's stereo have got to continually be on to be able to sense the channel. The main edge for a reactive jammer, nonetheless, would be that it might be more difficult to identify.

2.2 Security Goals

Security entails a set of investments which are properly funded. Inside MANET, most network capabilities including routing and packet forwarding are carried out by nodes themselves in a self organizing fashion. For these reasons, securing a mobile advertisement hoc system is incredibly demanding. The objectives to evaluate if mobile ad hoc network is protected or perhaps not are as follows:

- **Availability:** Availability means the property are available to authorized people at times that are appropriate. Availability applies both to information and also to services. It guarantees the survivability of community service despite denial of service attack.
- **Confidentiality:** Confidentiality guarantees that computer related assets are accessed solely by authorized parties. That's, just those who ought to have use of something will in fact get that access. In order to maintain confidentiality of a few confidential info, we have to have them secret from all entities which don't have privilege to get into them. Confidentiality is often known as privacy or secrecy.
- **Integrity:** Integrity suggests that assets can be modified solely by authorized parties or merely in authorized way. Modification consists of writing, changing creating, deleting, and status. Integrity assures that a statement actually being transferred isn't corrupted.
- **Authentication:** Authentication allows a node to make certain the identity of peer node it's talking with. Authentication is basically assurance that participants in interaction are authenticated and not impersonators. Authenticity is ensured because just the legitimate sender is able to produce a message that is going to decrypt right together with the shared key.
- **Non repudiation:** Non repudiation guarantees that receiver as well as sender of a statement can't disavow which they've previously directed or even received some email.This is useful when we have to discriminate whether a node with several undesired functionality is compromised or perhaps not.
- **Anonymity:** Anonymity means all info which may be utilized to recognize owner or maybe existing person of node must default be kept private and never be sent out by node itself or maybe the device application.
- **Authorization:** This property assigns various entry rights to various kinds of users. For instance a system management could be performed by network administrator just.

2.3 Taguchi's Loss Function

Taguchi's loss performance parameter design is an important technique to establish the perfect combination parameters. The primary goal is using Taguchi look for forecasting the greater details which can enhance the functionality metric over the setting of design details and minimize the sensitivity of the device efficiency to the cause of variation [6]. Taguchi parameter layout utilizes a unique style of orthogonal arrays (OAs) to learn the entire aspects with small amount of experiment only. The OAs enjoy a healthy home in which every parameter environment happens the exact same number of times for each setting of all the other parameters in

the experiment [6]. The OAs enables designers or researchers to learn numerous details concurrently and may be utilized to calculate the consequences of each parameter free from the additional parameters. Taguchi used a loss feature to compute the deviation in between the experimental worth as well as the preferred printer. The loss function differs for various objective functions. Usually, higher throughput and reduced the amount of routing overhead and packet fall are desire capable in ad hoc networks feature. Thus, to get optimum ad hoc community layout, the larger-the-better functionality metric for throughput have to be taken. (1)

3. Related Work

In this particular area we discuss about the prior job which has completed in the area of suggested investigate title.

Hossen Mustafa, Zhenhua Liu, Xin Zhang, Wenyuan Xu and Adrian Perrig in this particular work [7] examined multipath routing protocols which will respond to correspondence disturbance on demand. Particularly, a source node selects several various paths for reaching the location ahead of time. The accessibility histories of paths are well captured as well as calculated through availability history vectors. Leveraging AHVs, we've given 2 AHV based multipath selection algorithms: one selects numerous paths with the complete information of AHVs of the system, and also the various other computes the road in a distributed fashion. AHV-based algorithms may efficiently recognize several paths which provide high end-to-end accessibility, maybe even in the presence of a brand new jammer which didn't impact the system prior to track selection. Furthermore, the proposed distributed AHV based algorithm accomplishes greater availability than AODV in a smaller correspondence expense for long lived correspondence sessions.

Kwangsung Ju and Kwangsue Chung [8] Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi hop Tactical Networks In this tile, to conquer limits of the prior investigation, we suggest a brand new strong speed adaptation program that's resilient to jamming attack in a wireless multi hop tactical community. The proposed amount adaptation scheme detects jamming hit and selects the information transmission mode that has the expected maximum throughput according to the effective transmission probability. Through the performance evaluations, we show amount adaptation program which betters packet delivery ratio and the wireless link utilization.

Mr. Vinod Mahor, Sandeep Raghuwanshi in this particular work [9] offers the application of Taguchi's loss functionality strategy, a multi response optimization technique, for attaining much better overall performance during routing procedure of ad hoc on need distance vector (AODV) routing protocol. 7 parameters specifically terrain size, community size, quantity of energy sources, transmitted package rates, pause time, node speed, and transmission range are enhanced with considerations of several performance metrics like optimum packet delivery ratio as well as minimum routing overhead, end-to-end delay and packet fall. Based on a number of signal tonoise ratio (MNSR), maximum ph levels of variables are identified and substantial contribution of variables is driven by evaluation of variance (ANOVA).

Geethapriya Thamilarasu, Sumita Mishraand Ramalingam Sridhar [10] Improving Reliability of Jamming Attack Detection in Ad hoc Networks In this particular job, we concentrate on jamming style DoS strikes in the physical as well as MAC layers in 802.11 based ad hoc networks. Collisions in wireless networks occur on account of different things like jamming attacks, network congestion as well as concealed terminal interferences. We show a probabilistic analysis to demonstrate that collision occurrence by itself can't be utilized to conclusively determine jamming strikes in wireless channel. In order to boost the reliability of encounter detection, it's essential to offer enhanced detection mechanisms which could identify the particular reason for channel collisions. To deal with this particular, we 1st check out the issue of diagnosing the existence of jamming in ad hoc networks. We then assess the detection mechanism by using cross layer info from physical as well as link layers to distinguish between jamming and congested community scenarios. By correlating the cross layer information with collision detection metrics, we are able to differentiate hit scenarios from the effect of traffic ton on community conduct. Through simulation effects we demonstrate the usefulness of the scheme of ours in detecting jamming with enhanced accuracy.

Arif Sari and Dr. Beran Necat [11] Securing Mobile Ad Hoc Networks Against Jamming Attacks Through Unified Security Mechanism in this particular title we talk about used for stopping as well as mitigating jamming attacks is applied at the MAC level which include a mix of various control mechanisms. These're a mix of Point Controller Functions (PCF) which are utilized to harmonize whole community tasks in the MAC level as well as RTS/CTS (Clear-To-Send) systems that is a handshaking method which reduces the occurrence of collisions on the wireless community. The whole community efficiency as well as mechanism is simulated through OPNET simulation program.

G.S. Mamatha, Dr. S.C. Sharma, [12] Network Layer Attacks as well as Defence Mechanisms within MANETS a Survey In this particular title a report which will via lighting on this kind of strikes in MANETS is presented. The name additionally concentrates on various protection factors of community level and also covers the outcome of the attacks in detail by way of a a survey of tactics employed for protection job.

Rajeev kumar, Anshuman kr. Saurabh [13] An evaluation on movable Ad hoc Network and also attacks Happened at Different Layers The primary target in this particular name is on attacks security measures at different levels within MANET. Which stop attacks as well as hit take place in MANET because protection would be the most dominating element.

CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma [14] Security Challenges as well as Attacks in Mobile Ad Hoc Networks This name offers an extensive analysis of attacks against mobile ad hoc networks. We show a comprehensive classification of the attacks against MANETs.

4. Proposed Method

Please In this particular job we are going to made a crucial observation that absolutely no measurement is adequate to reliably classify jamming strike. We develop the job of ours on the foundation of the observation and create a detection as well as prevention mechanism which eliminates the ambiguity in detecting jamming from congested scenarios. In this particular job, we are going to focus on detecting jamming attacks which happen during each MAC levels as well as network level of an 802.11 ad hoc system. We show a distributed checking mechanism to select monitor nodes accountable for identifying channel accessibility. The proposed protection program has the ability to deal with the jamming hit situations and solve the issue of link blockage from jamming. Taguchi's loss functionality is discovering the factors which degrades the network performance as network size, nodes etc. These elements are degrades the overall performance as a result of arbitrary deployment of movable nodes in area that is big or maybe tiny area but in case we handles these variables through changing in various elements that is ideal and in favor of network quality it means the system efficiency is enhances at that conditions well then Taguchi's loss functionality is vitally important. The implementation program of proposed job is mentioned below.

Protection is a vital requirement of MANET. With no appropriate security solution, the malicious node in the system is going to act as a typical node that causes major flooding of this particular flooding and command packets is begin to a couple number of packets and after a while the substantial amount of packets are flooded in network usually referred to as jamming strike. In this particular analysis we are going to proposed the protection program against jamming happened in the in MANET. Jamming hit is among the attacks in MAC level in terminology of channel access, bandwidth allocation and also in community level in terms of packets. This particular strike is comes under protection established strikes in MANET. The Taguchi's loss functionality is calculated that which element (like mobility, community region, amount of nodes etc.) is impacted the functionality of system after using protection scheme.

5. Sampling Design

Jamming attack can be accomplished remotely and locally, and it's among the most typical types of protection attacks, since it will take just frequent and affordable online resources, and doesn't need significant technical information. The flooding packets as well as sophistication of packets are quickly increasing based on a few techniques such as direct active attacks. This kind of security risk which stops authorized owners from getting permission to access the wireless channel by disrupting community operations, affecting community connectivity and accessibility. The primary difficulty of network is the fact that you can get several aspects as nodes mobility, amount of nodes as well as transmission range may also be impacted the functionality of network and on account of which reason the efficiency is degraded far too much isn't examined person. The security program is defend the system from attacker however, if to solve the wreckage from some other element is definitely the significant problem issue in MANET.

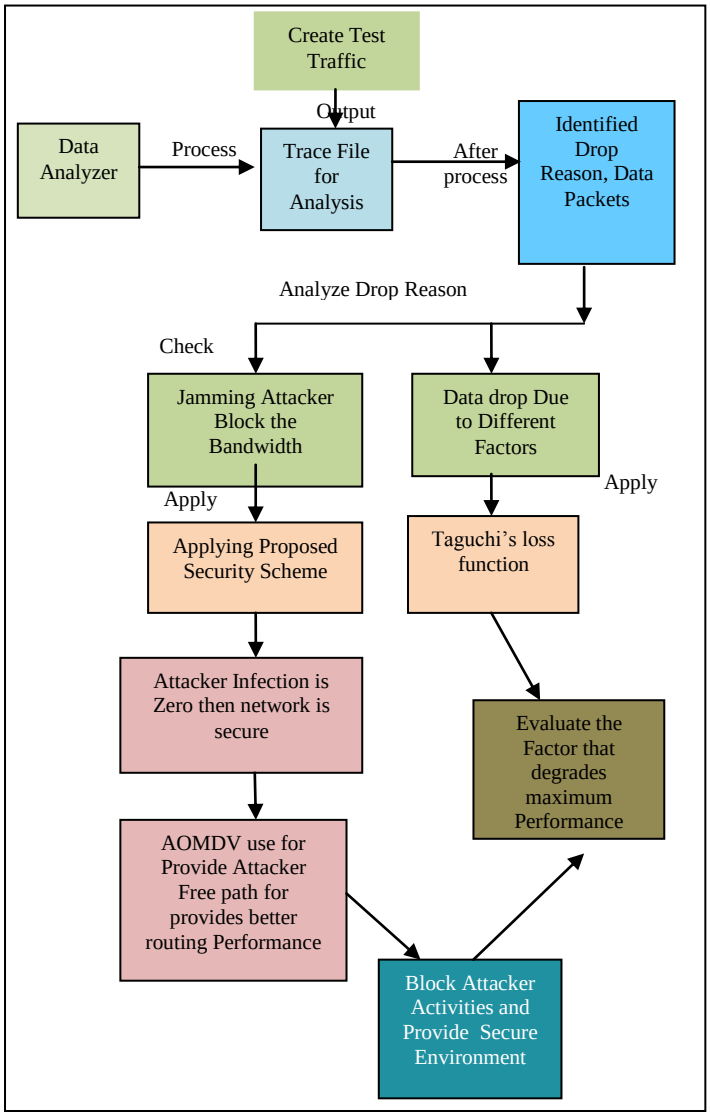

Figure 2: Architecture of Proposed Work

Each mobile node functions as a host when requesting/providing info from/to alternative nodes within the system, and also functions as router when maintaining and identifying routes for remaining nodes in the system. Taguchi's loss function in a position to measured the factor which degrades the system performance. The proposed program will certainly gets better the system performance i.e. measured through performance metrics and also offers the zero percentage infection after using the security program against jamming attack. Taguchi's loss function is used after security scheme against jamming assault and also the network shows is calculated in various community element and enhance that aspect in network that is secure.

6. Data Collection Strategy (Primary & Secondary Methods)

For data collection as well as implementation we are going to use Network Simulator- two (NS-2). The description regarding simulation environment can be as follows:

Network simulator two (NS2) could be the consequence of an on going work of study as well as advancement which is administrated by researchers at Berkeley [sixteen]. It's a discrete occasion simulator targeted at networking studies. It offers considerable support for simulation of TCP, routing, and also multipath protocol.

The simulator is created in C++ as well as a script language known as OTcl. Ns use an Otcl interpreter towards the computer user. It means that the person creates an OTcl software which describes the system (number of nodes, links), the visitors in the network (sources, destinations, kind of which protocols and traffic) it'll make use of. This particular script will be used by ns throughout the simulations. The outcome of the simulations happens to be an output trace file which may be utilized in order to do information processing (calculate delay, throughput etc) and then to imagine the simulation with a system named 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 category hierarchy is instantly developed through techniques identified in the category Tcl Class. operator instantiated objects are mirrored through methods defined in the class Tcl Object. There are some other hierarchies in the C++ code as well as OTcl scripts; these various other hierarchies aren't mirrored in the fashion of Tcl Object. To be able to setup the simulation system for ns2, you have to make use of a language known as Tcl. It utilizes an extension of Tcl, known as OTcl, that features items into Tcl. access an interactive OTcl timely by operating the ns command (from a Linux shell or maybe Cygwin on Windows, for example).

7. Simulation Strategy

NAM is a very good visualization tool that visualizes the packets as they propagate through the network. An overview of how a simulation is done in ns is shown in Figure 2.

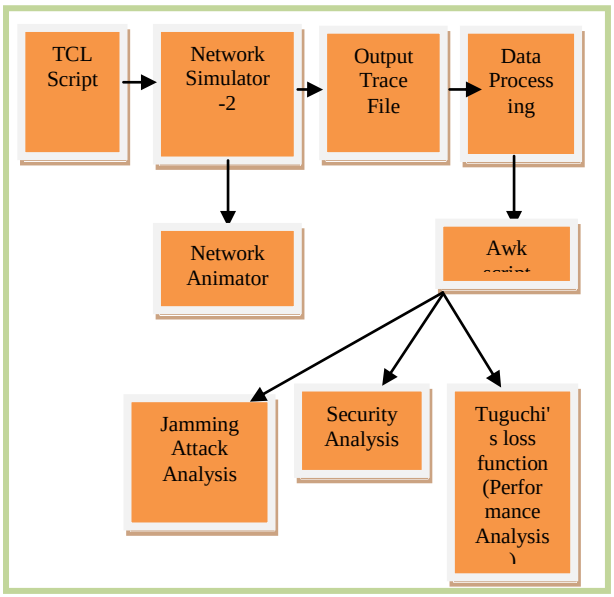

Figure 3: Simulation Strategy

8. Planning Of Analysis of Data

We get Simulator Parameter as Number of nodes, Routing protocol, Dimension, traffic etc. Based on below table 1 we simulate the network of ours.

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

8. 1 Performance Measure

The following general performance matrices are used to determine the overall performance against jamming assault and determine the performance elements through Taguchi's loss feature which improves network efficiency.

- **Packet Delivery Ratio:** The ratio in between the quantity of packets originated by the application level CBR resources and also the selection of packets obtained by the CBR sinks in the last location.
- **Average End-to-end Delay:** This includes all of the possible waiting times due to buffering during route discovery latency, queuing in the user interface queue, retransmission delays at the MAC, and also propagation as well as transfer times.
- **Packet Dropped:** The routers could possibly fail to provide or maybe shed several information or packets in case they turn up when the buffer of theirs happen to be complete. A few, none, or maybe all of the packets or information could be dropped, based on the state of the system, and it's not possible to find out what'll take place in advance.
- **Routing Load:** The entire amount of routing packets

transmitted throughout the simulation. For packets delivered over several hops, each transmission of the package or maybe each hop matters.

8.2 Practical Approach

For deployment of protected wireless ad hoc community the mobile devices are utilized that support MANET routing capability for that purpose we utilize Android based devices and built-in the module of ours into android based phone and stop the MANET and also enhance the quality of service of the system, but recognize one day MANET achievable products unavailable on the market.

8.3 Application for Society

Movable ad hoc community of recent trends unavailable in which it's completely deployed therefore offer completely free correspondence networking which reduce the price of service provider, very easily any where public speak without having the demand of infrastructure, which will help emergencies scenario wherein infrastructure not exist.

9. Conclusion and Future work

MANETs provide a chance of producing a system in situations where producing the infrastructure will be not possible or prohibitively expensive. Compared with a system with fixed infrastructure, movable nodes in ad hoc networks don't speak through entry points (fixed structures). Each movable node functions like a host when offering or requesting info from or even to various other nodes in the system, and also functions as router when maintaining and identifying routes for various other nodes in the system. Taguchi's loss functionality ready to measured the component that degrades the network efficiency.

The upcoming simulation of suggested scheme will certainly improves the network efficiency i.e. measured by performance metrics and offers the zero portion infection after using the security scheme against jamming strike. Taguchi's loss functionality is used after security pattern against jamming assault and also the system performances is calculated in various community element and enhance that element in network that is secure.

References

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. http://www.isi.edu/nsnam/ns/

