International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 7, Issue 2, March - April 2018 ISSN 2278-6856

# Secure and Authenticate Jamming Attack Proof Secure Information Transmission in Mobile Adhoc Network

**Harsha Jain[1], Pranita Jain[2]**

[1] Department of Computer Science Engineering,
SATI College, Civil Lines, Vidisha, M.P., India

[2]Department of Information Technology,
SATI College, Civil Lines, Vidisha, M.P., India

**Abstract— An Ad-hoc mobile network is an assembly of wireless transportable nodes devotedly creating a short-lived network lacking the use of any core-existing centralized administration or network infrastructure. MANET have restrictions owed to mobility, capability and infrastructure of mobile systems nodes because of network system as an entire. Limitations due to system or infrastructure, Limited bandwidth, Broadcast nature of communications, variable capacity link, frequent disconnections/partitions, packet loss due to transmission error. Cooperative procedures, Exposed medium, Dynamically varying system topology, Inadequacy of centralized monitoring, Nothingness of clear line of opposition. There is no layered safety in MANETs like in wired network. Experimentally conclusion point out that system is fine suitable for superior and convinced data communication. Directing set of rules of Ad-hoc network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. The outcomes showed that the system throughput and security of the system is improved. This paper recommends an innovative methodology to prevent and detect the jamming based attack and equally preserve harmless the network from malicious machines. The system organization also achieved safe routing to defense MANET against malevolent machine.**

**Keywords—** MANET, Wireless communication, Routing, Node Security, Jamming attacks

## 1. INTRODUCTION

In MANET [1] the mobile wireless network is not rely on any existed network. It is a combination of several wireless nodes that can build a network randomly. The study and growth of mobile devices and 802.11[2] Wi-
Fi wireless networks is on demand topic of research in MANET. Ad-hoc network doesn't depend on any central supervision or constant infrastructure[3] such as base. Even as system nodes are moving in the system they swap the information to every other and may keep on to be in motion there and here and so the network should be prepared. Mobile system devices are not have the central control, consequently they are liberated to be in motion, and thus the topology of such system network changes expeditiously. In the mobile Adhoc system, a number of influences such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the lifetime of a link[4] among two mobile nodes. The superiority of service should meet the terms source system end to destination system end data packet transfer without packet loss. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links[5], which is known as the multihop path.

To accomplish availability and reliability [6] network routing protocols should be prevailing compared to jamming attacks[7]. The honesty of distribute information packets from system end to end with the help of multihop mediator nodes is a remarkable dilemma in the mobile Adhoc network. Because of the inherently self-motivated nature of the mobile system network layout, the prevailing data routes cannot be secure. Determination of information safety measures, link malfunction, exposure of malevolent node and protected information transmission within MANET is a significant tasks in any mobile network.The paper emphases on the following problem: Detection, prevention and correction of jamming attack in multipath [8] mobile Adhoc network and to increase performance and trustworthiness of mobile Adhoc network under jamming malicious attack with secure data transmission and routing.

The main aim is to notice secure route of the mobile network, to progress the information delivery ratio and performance of MANET, to select best transmit path for safe and sound information transmission. Detection of attacks, data security[9], detection of malevolent node and protected information transmission in a MANET is an imperative tasks in mobile network. Recognition of malevolent node, data Security within a MANET is an central task in any network.

The objectives are to detect jamming attacks in MANET, to prevent MANET from jamming attack, To improve the performance of network.The system proposed a secure trust value[10] which helps authenticate the system node and also remain protected the network from malicious nodes

The system also perform secure routing to protect MANET against malicious node. The proposed protocol discover the jamming based attack and if original link is breakdown then new secure node is established and information is transferred from newly created link. Experimentally result showed that scheme is well suited for better data transmission. The system also perform secure routing to protect MANET against malicious node.

The rest of the paper is organized as follows.

Section 2 represents literature survey related to jamming prediction, detection and failure. Section 3 provides proposed work and algorithm. Section 4 provides the implementation details of the proposed work. Section 5 concludes the paper with a summary of the work and discussion of future research directions.

## 2. LITERATURE SURVEY

Jamming attack is a kind of DOS attack[11]. In jamming attack a radio signal can be interfered or jammed. The jamming attack may corrupt or loss the message and disturb the communication.

Jamming attack may increase the packet drop ratio[12] which means total quantity of dropped packets to the quantity number of directed packets.

In jamming attack the attacker is flooded[13] the large variety of unwanted packets within the network to consume network resource.

The attacker will transfer every bit directly, while not waiting the whole packet. It's terribly tough to seek out the placement of part attack while not having the crypto logic key[14] or while not glorious infrastructure of routing protocols.

A jammer can easily designed by attending to the shared wireless medium and transmitting in the similar bandwidth as system network, without necessity of specific hardware device.

As jamming attacks poorer the performance of mobile adhoc network, some effective approaches are required to perceive their existence.

Numerous metrics[15] are used to describe jamming attacks in a network. The jamming attacks metrics are packet sent ratio, signal strength, carrier sensing and packet delivery ration.

Packet sent ratio, is calculated at the node transmitter side, is the entire number of acknowledgments data packets received[16] to the entire number of data packets communicated.

Carrier sensing time[17] can be understood as the period when a machine has to wait for the wireless channel to get quiet to start its data transmission.

Signal strength is intended power that is evidently seen on the receiver side.

Packet delivery ratio denotes to the ratio complete number of data packets appropriately received to the over-all number of data packets received.

As the foundation of other mobile system network processes such as routing and medium access control, safe neighbor detection[18] need be regularly achieved due to node mobility. Traditional anti-jamming transportations frequently be determined by on spread-spectrum systems, which all necessitate that the interactive gatherings use a common extent code (unidentified to the opponent) to spread the signs such that the communications are random and thus tough to jamming. The open wireless medium in MANETs renders secure neighbor discovery particularly vulnerable to the jamming attack, in which the adversary purposely communicates noise-like signals to avoid neighboring nodes from switching messages and thus discovering each other.

In the mobile Adhoc system, a number of effects such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the link failure of a link among two mobile nodes. To achieve availability, security and reliability routing protocols should be powerful against malevolent attacks[19]. Because of the fundamentally enthusiastic behavior of the mobile system network binding topology, the obtainable links are frequently damaged, and additional links are frequently recognized. Detection[20] and correction of attacks to increase performance and trustworthiness of mobile Adhoc network using dynamic source routing under malicious attack with secure routing and data transmission. The excellence of data service should justify source end to destination end information packet transfer without packet loss.

The proposed protocol discover the jamming based attack and if original link is breakdown then new secure node is established and information is transferred from newly created link The aim is to detect secure route of the mobile network, to progress the information delivery ratio and performance of MANET, to select best route for secure data transmission. To improve the information delivery ratio and MANET performance and also detect and correct attacks is the main problem in MANET. Mobile Adhoc network needs safety and consistency of data packets. Real time applications in MANET require certain QoS structures, such as acceptable data loss and minimal end-to-end packet delay. Detection of secure route of mobile machines with the assistance of transmitting information is also problematical in an MANET because of its real time[21] moving topology.

## 3. PROPOSED METHOD

Determination of link failure, detection of malicious node, data safety and protected information transmission in a MANET is an imperative task in any mobile system network. The proposed algorithm is exemplified in this fragment. This algorithm provided all the steps of proposed work. The proposed algorithm will jamming based attacks in the mobile system and informed to the mobile network. The proposed algorithm discover the jamming based attack

and if original link is breakdown then new secure node is established and information is transferred from newly created link. The packet drop and delivery ration is also tested to discover system performance of the network.

**Algorithm**

1. Threshold value setup for PDR
2. Send route request to initiate data transmission
3. Check signal strength, carrier sensing time of the requested neighbor

If all parameter tests are above threshold value then
    Neighbor is valid path can be established
    Node can transmit data to neighbor
Else if system hop sum total exceeded with initial hop then
        Network is invalid
        Stop transmission and Goto End
Else
    Goto step 2 and make route request to another neighbor
End if

4. Check packet drop and delivery ratio of the network system

Is packet delivery ratio fall to the given threshold value then
    Source machine arbitrarily pick out the next neighbor
Is any neighbor node reply from new route excepting neighbor node then
    Initiate the inverse locating mechanism and direct test hello packets
Read replay messages to detect jamming attack
Initiate node list disagreed node onto malicious list
Alarm packet is initiated
Goto Algo End
If End
End Algorithm

The description of the proposed algorithm is as given below. The first stage in suggested work is to initialize threshold values for packet drop and delivery ratio to identify jamming attack in the network. We also fixed the packet size, routing parameters, dimensional area, routing protocols, and rate of transmission. Send route request to initiate data transmission. Check signal strength, carrier sensing time of the requested neighbor if all parameter tests are above threshold value then neighbor is valid path can be established. Node can transmit data to neighbor. Otherwise system hop sum total exceeded with initial hop then network is invalid stop transmission and end the data transmission. Then make route request to another neighbor. Check packet drop and delivery ratio of the network system if packet delivery ratio fall to the given threshold value then source machine arbitrarily pick out the next neighbor. Is any neighbor node reply from new route excepting neighbor node then initiate the inverse locating mechanism and direct test hello packets. Read replay messages to detect jamming attack. Initiate node list disagreed node onto malicious list alarm packet is initiated.

## 4. IMPLEMENTATION

For simulation environment used i5 2.4 GHz computer system with 8GB RAM. The implementation script is written in TCL scripting language and a few procedures are also scripted in C++/C language. NS2 is applicable as simulation environment. In implementation scenario, simulation network used 50 system nodes, which are at random placed in unlike parts of position division with a stationary density. For this implementation scenario, simulation network parameters, transmission range, such as traffic, Dimension, Number of nodes, transmission rate, sensitivity, transmission power, Routing protocol, etc., are used.

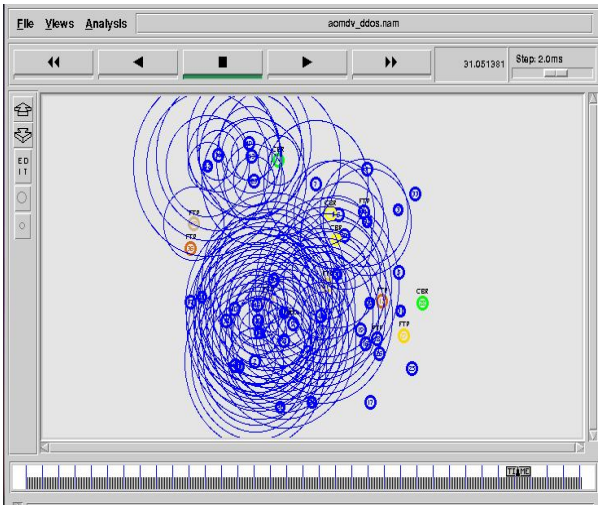


**Figure 1**: Jamming attack in network

In this Figure represents the Jamming attack in a network. Jamming attacks breakdown the network and links to the different nodes are damaged.

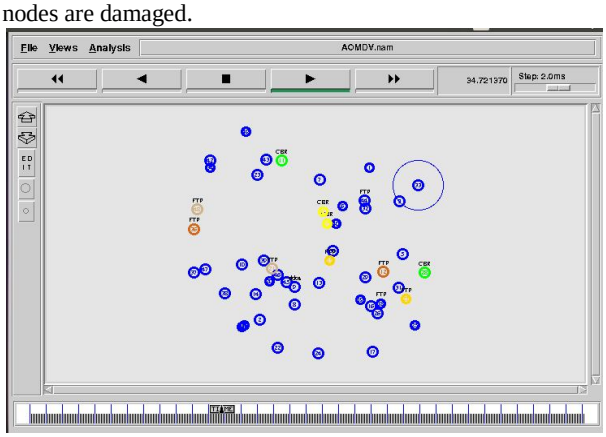


**Figure 2**: Jamming attack prevention

In this Figure represents the prevention of Jamming attack using detection node.

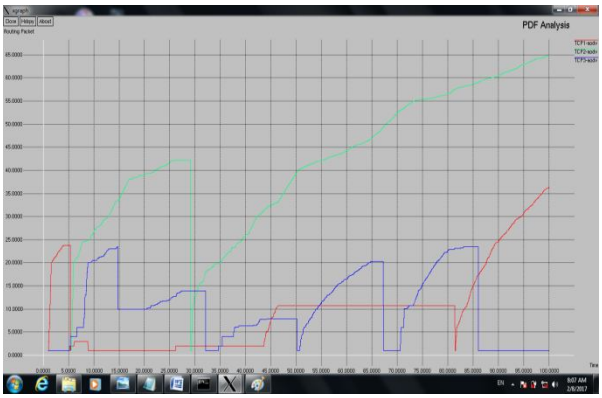


**Figure 3**: PDR Analysis

In this graph Packet Delivery Ratio(PDR) performance of Jamming and security scheme is describe in this graph. Packet sent ratio, is calculated at the node transmitter side, is the entire number of acknowledgments data packets received to the entire number of data packets communicated. By Jamming attacker technique the attacker drop of packet is humiliates the percentage ratio of data receiving. Before the attacker drop of packets is maximum and after using Jamming attacker the drop of packets ratio is minimum.

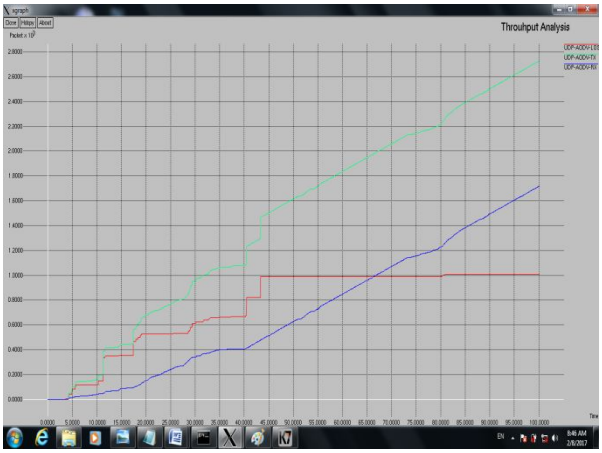


**Figure 4**: Throughput Analysis

In this graph Throughput Analysis of Jamming and Security Scheme the attacker aim is to drop the data packets or to hold the resources for that the communication is affected. The packets forwarding capacity of jamming is a strictly increase with period of time. Overall related work the packets ratio drop is maximum and security are minimum and proposed work the packets ratio in minimum drop and and security is maximum.

**Table 1**: Neighbor discovery probability after jamming attack

| Probability | Number of compromised nodes | |
|---|---|---|
| | M-NDP | Our method |
| 0.2 | 38 | 31 |
| 0.4 | 30 | 24 |
| 0.6 | 25 | 20 |
| 0.8 | 14 | 12 |
| 1.0 | 6 | 5 |

This table represents the neighbor discover probability after jamming attack. As number of compromised nodes increases the neighbor discovery probability decreases. In our method due to jamming attack prevention neighbor discovery probability improved.

**Table 2**: Neighbor discovery latency after jamming attack

| Propagation range | Latency | |
|---|---|---|
| | M-NDP | Our method |
| 0.5 | 0.8 | 0.5 |
| 0.6 | 0.9 | 0.6 |
| 0.7 | 1.1 | 0.8 |
| 0.8 | 1.3 | 0.9 |
| 0.9 | 1.6 | 1.0 |
| 1.0 | 1.7 | 1.3 |
| 1.1 | 1.9 | 1.5 |
| 1.2 | 2.1 | 1.8 |

This table represents the latency after jamming attack. As number of compromised nodes increases the latency is also increases. In our method due to jamming attack prevention latency is improved.

## 5. CONCLUSIONS

The study and growth of mobile devices and 802.11 Wi-Fi wireless networks is on demand topic of research in MANET. Real time applications in MANET require certain QoS features, such as tolerable information loss and nominal end to end information packet interval. AODV set of regulations is a wise protocol in wireless mobile ad-hoc network. Because of the instinctively enthusiastic nature of the variable topology, the existing paths cannot be protected. MANET network using AOMDV under jamming malicious attack with secure routing and data communication. The implementation outcome revealed that the system throughput, security and system performance is enhanced. The proposed protocol discover the jamming based attack and if innovative direction is interrupted then diverse confined system node is accepted and information is communicated from freshly twisted path. The paper proposed detection and correction of jamming attack in MANET and to increase performance and trustworthiness of mobile Adhoc network under malicious assault with convinced routing and information communication. The proposed scheme is well appropriate for mobile network security. The proposed system is planning to implement in real environment and evaluate the network performance. A direction of upcoming exploration is to use better encryption scheme to secure data transmission in jamming attack.

REFERENCES

[1] Amit N Thakre, Mrs. M.Y.Joshi “Performance Analysis of AODV & DSR routing Protocol in

Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network" MANETs 2010.

[2] A. Feldmann, A. Gilbert and W. Willinger, "Data networks as cascades: Explaining the multifractural nature of internet traffic", in Proc. ACM SIGCOMM, Sep 1998, pp.42-55

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE 2002, pp-433-445

[4] P. Barford, J. Kline, D. Plonka, and A. Ron, " A signal analysis of network traffic anomalies", in Proc. ACM SIGCOMM Internet Meas, Workshop France, 2002, pp. 71-82

[5] Josh Broch , David A. Maltz , David B Jhonson, Yih-chunhee, Jorjeta Jatchene, " A Performance Comparison of Multi-Hop Wireless Ad-hoc Network Routing Protocol", Computer Science Department Carnegie Mellon University Pittsburg PA 15213, Available at http://www.monarch .cs.cmu.edu/

[6] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[7] R. Zhang, Y. Zhang, and X. Huang, "JR-SND: Jamming-resilient secure neighbor discovery in mobile ad-hoc networks," in *Proc. IEEE ICDCS*, Minneapolis, MN, USA, Jun. 2011, pp. 529–538.

[8] Rui Zhang, Jingchao Sun, Yanchao Zhang, and Xiaoxia Huang, Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, NO. 10, OCTOBER 2015, pp.5588-5602

[9] T. Jin, G. Noubir, and B. Thapa, "Zero pre-shared secret key establishment in the presence of jammers" in *Proc. ACM MobiHoc*, Apr. 2009, pp. 219–228.

[10] Antesar M.Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2114

[11] G.Macia-Fernandis, J. E. Dias and P.Garcia-Teodoro, "Mathematical Model for low-rate DoS attacks against application servers, "IEEE Trans. Inf. Forensics Security, Vol. 4, no.3, Sep. 2009, pp. 519-529.

[12] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, "Defending DSSS based broadcast communication against insider jammers via delayed seed-disclosure," in *Proc. ACSAC*, Austin, TX, USA, Dec. 2010, pp. 367–376.

[13] P.Papadimitratos*et al.*, "Secure neighborhood discovery: A fundamental element for mobile ad hoc networking," *IEEE Commun. Mag.*, vol. 46, no. 2, pp. 132–139, Feb. 2008.

[14] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE S&P*, Berkeley/Oakland, CA, USA, May 2008, pp. 64–78.

[15] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. USENIX Security*, Aug. 2009, pp. 231–248.

[16] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun. Surveys Tuts, vol. 15, no. 4, pp. 2046–2069, Fourth Quarter 2013.

[17] Z. Xia, S.Lu and J.H. Li, "DDoS flood attack detection based on fractal parameters", Proc. 8th Int. Conf. Wireless Communication Network Mobile Computing, 2012, pp1-5.

[18] H Yan-Xiang, C. Qiang L. Tao, H. Yi, and X.Qi, "A low rate DoS detection method based on feature extraction using wavelet transform", J. Soft, Vol 20, no.4 pp. 930-941, Apr. 2009

[19] U.Venkanna, R. LeelaVelusamy, Mitigating the Attacks on Recommendation Trust Model for Mobile Ad Hoc Networks, IEEE 2015, pp 223-234

[20] Wenjia Li, Anupam Joshi, Tim Finin, CAST: Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies, IEEE 2010, pp-188-201

[21] Charlos De Cordeiro and Dharma P. Agarwal " Mobile ad-hoc networking",OBR Research Centre for Distributed and Mobile Computing, ECECS, University of Cicinnati –USA.