# A Weighted Probablistic Model for Preventive Route Formation against Man-In-Middle Attack

**[1]Sarita Choudhary, [2]Prof. Dr. Ajay Khunteta**
[1]Student, M.Tech. (CSE) , [2]Professor, Dept. of CSE
[1]Name of Department of 1st Author,
[1,2]Poornima College of Engineering, Jaipur, Rajasthan, India

***Abstract*—The global communication feature of mobile network increases the security threat in this network form. The internal or the external nodes can participate in the network to disrupt the communication and to increase the network QoS. One of such attack is open mobile network is Man-in-the-middle attack that captures the communication and increases the communication loss. In this paper, a weighted probabilistic model is presented to provide reliable and safe communication. In first stage of this model, the featured analysis at node level is performed to distinguish the attacker and the safe node. In second stage, the session specific probabilistic estimation is applied to identify the safe communication path. The simulation results signify that the model has improved the network communication and reduced the communication loss.***

***Index Terms*—MANET, Man-in-the-Middle, Probabilistic, Weighted**

## I. INTRODUCTION (HEADING 1)

A Mobile network is the public network deployed randomly and provides the dynamic communication formation. The lack of infrastructure enables the cooperative network communication that increases the network flexibility but also affects the security constraints of the network. The network suffers from different kind of internal and external attacks that affects the communication in different way. The common attack form, in cooperative communication is identified as Man-In-the-Middle attack. To provide the end-to-end user communication between the users, the distribution control is provided by IEEE 802.11. It provides the broadcast specific security vulnerabilities analysis so that the communication will be effective within range and reliable and adaptive communication will be performed. The data nature specific analysis is here provided to the security measurement so that paired communication will be performed. The frame check specific analysis is defined with inclusion of different access points. Here the common form of Man-in-the-middle attack is shown in figure 1

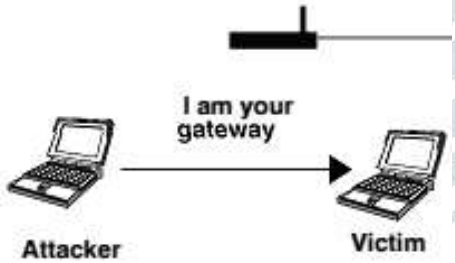


Figure 1 : Man-in-the Middle Attack

Here figure 1 is showing the common working of man-in-the-middle attack. As shown in the figure, the attacker behaves as the some other node in the network and captures the network communication. It provides the fake id based on which the communication is diverted to that node and the actual receiver does not get the communication data. Some of the common attack forms are defined in this section

***A) Wormhole Attack***

This particular attack creates a virtual tunnel between two nodes so that the communication revolves between these nodes. Each of the attacker node, communicate effectively with the tunnel node but does not perform any communication or data forwarding to any other mobile node. The interaction ratio of the wormhole node is high with other wormhole node but very low with other any healthy node.

***B) Blackhole Attack***

This kind of attacker captures the network communication and does not allow the packet forwarding. The node presents itself as the sink node and receives the communication from all the network nodes. This attack results heavy communication loss because of negligible forwarding.

***C) Rushing Attack***

The particular attack is the tunnel specific attack defined with specific node pair. The communication between the nodes is not effective. The tunnel formed between two end nodes performs the fast communication. It is a form of DDOS attack that basically slows down the communication and degrades network QoS

In this paper, a probabilistic weighted approach is defined to identify the man-in-middle attack. The model first applied the node level analysis under multiple parameters and assigned weights to each node. Later on the probabilistic evaluation based node selection is done for the communication. In this section, the basic threats to the mobile network are identified with exploration of Man-in-the-middle attack. In section II, the work provided by earlier researchers is discussed. In section III, the research methodology is provided relative to the work. In section IV, the results obtained from work are presented. In section V, the conclusion of work is presented.

## II. RELATED WORK

The work is here defined to provide the preventive communication against Man-In-The-Middle Attack in MANET. The works defined by earlier researchers are defined here in this section. Kumar et. al.[1] has defined a work on to detect the Stealth Man-In-The-Middle attack in

WLAN network. Author used the structural analysis with key management to identify the attack in the network. Author implied a probe response handler to recognize the positive and negative response in the form of attacks. Sandhya et. al.[2] has identified the Man-In-The-Middle attack for contention control in Bluetooth network. Author proposed a new association specific pairing model for attack detection. Based on these pairs the link key estimation and relatively encoded communication is provided by the author. Author implied the security in application layer of the communication. Tang et. al.[3] has used an intrusion detection system against the TCP adaptive flooding control as Man-In-The-Middle Attack. Author defined an architectural solution by setting up some analytical rules to identify the attack. The framework is based on requirement observations and relatively provides the secure communication in the network. Chen et. al.[4] has defined a mutual mapping to the node by applying the mathematical model against Man-in-the-Middle attack. Author applied the investigation with specification of shared key map so that SSL based encoded communication is performed. An exclusive attention based analysis was defined to provide reliable communication by applying the cryptography methods. Bicakci et. al.[5] has defined a new authentication protocol to provide reliable communication in mobile network without relying the communication. The secure element specific incorporated communication was defined with context information specification. Author processed the connected services with specification of message server and existence of the ongoing attack. Author processed the genuine service provider for attack detection and provided the reliable key shared communication. A signature adaptive secure communication was provided by the author for mobile network.

Chen et. al.[6] has defined a framework for Man-in-the Middle attack detection in wireless network. The provided unified mathematical model analyzed relationships, propositional analysis and operational mapping to identify the abnormality in the network. The logical reasoning based attack detection method is provided. The method removed the vulnerability in the network and improved the network communication. Meyer et. al.[7] has used the GSM encryption based attack detection based on interoperating node specific analysis. Author provided the encoded communication for UMTS connection as well as a key agreement based intersystem for reliable handover is provided. The key transformation based authenticated measures are applied to communicate only with reliable nodes. Zhang et. al.[8] defined a gateway based protocol to control the packet and circuit switching to identify the eavesdrop in the communication network. Author analyzed the communication pattern using probabilistic measure to identify the attack. The performance measure specific attack detection model is provided to provide safe communication in the network. Haataja et. al.[9] has defined a two particle based Man-In-the-middle attack detection in blue tooth network by applying the paired security. The attack devise counter measures are suggested by the author to render the attack and generate the safe communication path. A capability driven analysis with key exchange method was provided to obtain safe communication links. The security algorithm is also implied on the centralized device to provide safe and reliable communication. Haataja et. al.[10] also provided a comparative study on different type of attacks, their impact and countermeasures. The association model based on device capability was provided by the author to generate the encoded communication. Author discussed the association specific reliable communication modeling with existence of fatal error and usability constraints to improve the network reliability. Fayyaz et. al.[11] has defined a preventive method for man-in-the middle attack detection in network environment. The seed based multi-generation method was provided to track the packet forwarding. Author provided the ARP poisoning to provide the tracking to victim cache and identify the fake packet delivery.

Galluccio et. al.[12] has focused his work on control center driven node tracking in personal interest and provided the diversion attack i mobile network. The energy consumption and relative security adaptive feature tracking was proposed by the author. The security and the feature map based metrics processing was defined analyze the radio coverage. The reader specific modeled information was process to identify the communication errors or the packet failure. The flow specific analysis identified the hidden transmission to improve the network reliability. Agarwal et. al.[13] has defined the attack detection in encoded communication in WiFi network. Author also identified the attack constraints including the attack life, tougher detection ratio and the degree of attack. Author identified the challenges relative to the communication and the attack and generated the safe communication. Nayak et. al.[14] has identified different flavors of man-in-middle attack along with consequences and feasible solutions. The attack constraints and communication patterns were observed with specific communication analysis to classify the normal and attack instances. An authentication mechanism with DNS poisoning was analyzed as the gateway operated framework in which certificate check is performed at initial level. The sniffing based communication is analyzed to generate the safe communication. Nam et. al.[15] has used the preventing communication with incremental deployment. The switch specific diversities and the rule specific channel allocation are provided in this work.

## III. RESEARCH METHODOLOGY

A Mobile network is the public network in which cooperative communication is performed by generating the dynamic path. These intermediate communication nodes can be normal nodes or the attacked nodes. The attacker node captures the network communication or includes some kind of disruption so that the communication loss, energy loss or the quality of service degrades. To provide the reliable communication in mobile network, it is required to detect the attacker node and generate the preventive communication over the network. In this present work, a probabilistic and weighted method is provided against the Man-In-Middle attack. The work is here divided in terms of three integrated stages. In first stage of this model, the node level weighted analysis is performed to assign the weights to node based on the reliability. The parametric analysis is here performed based on three main parameters called delay analysis, loss rate analysis and the communication analysis. The loss rate parameter is able to identify the communication capturing or diversion. The delay parameter is here defined to identify the irregularity in communication based on which the attack can be identified. The rate level estimation is also applied to identify the abnormality in the flow of communication. Once all the parameters are collected for each node, these parameters are combined with some weighted measures. As the generalized form, the equal weights to all the feature vectors are assigned. But in some particular attack, the weights can be modified to identify the specialized attack form. Such as, in case of DDOS attack the delay vector will be defined with higher weight. In second stage of this model, the probabilistic aggregative estimation is applied to identify the attacker node. The flow of the proposed work model is shown here in figure 1.

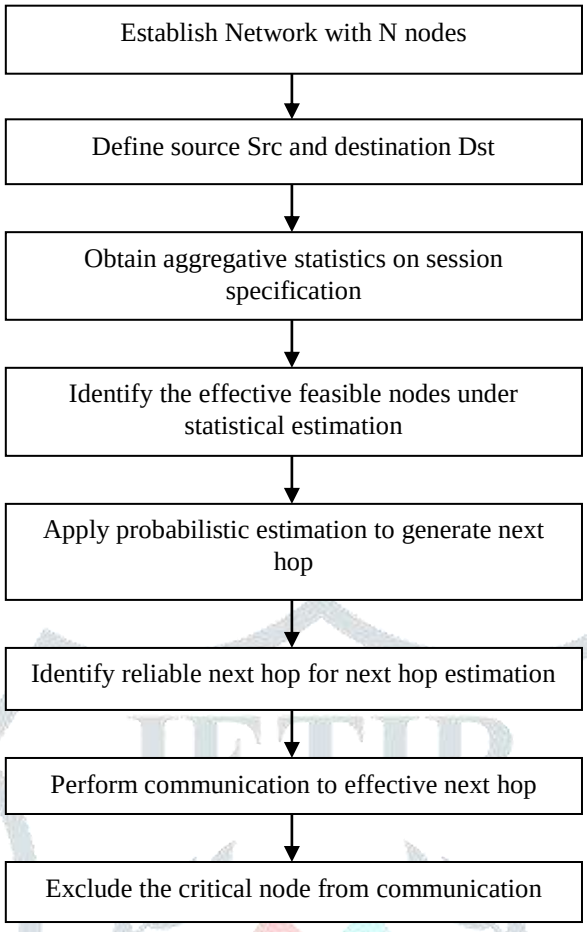


Figure 1 : Proposed Work Model

Here figure 1 is showing the work flow of proposed algorithm. According to this proposed model, the network is defined at random position with specification of dedicated communication nodes. To perform the attacker and safe node detection, the weighted analysis approach is defined. The evaluation of each node is done under three main communication parameters. To obtain the probabilistic aggregative analysis, the session specific communication observation is taken. This analysis is here done at parameter level and node level. At first level, the feasible nodes are identified based on coverage map and the communication response analysis. In second stage, the communication parametric evaluation for the session is obtained. In third stage, the session specific probabilistic weighted evaluation is performed to distinguish the attacker and the safe node. Finally, the most effective neighbor is identified over which the next communicating is performed. This hop by hop node selection is performed till the effective packet delivery is not done. The work is implemented in NS2 environment with random scenario and the observations are taken against multiple parameters. The analysis results are shown in next section.

## IV. RESULTS

The presented research has provided a probabilistic weighted method to identify the man-in-middle attack and provided the safe communication over the network. The work is applied on a random scenario and conducted the simulation in NS2 environment. The network parameters relative to the defined scenario are listed here in table 1.

Table 1 : Network Parameters

| Parameters | Values |
|---|---|
| Network Coverage | 100x100 |
| Topology | Random |
| Mobile Nodes | 36 |
| Routing Protocol | AODV |
| Packet Size | 512 Bytes |
| Simulation Time | 100 sec |
| MAC Protocol | 802.11 |
| Initial Energy | 20J |
| Transmission Loss | .3J |
| Receive Power Loss | .3J |

The table has showed the parameters of scenario considered here for the simulation. The results are generated in terms of communication loss, communication throughput and delay parameters. The comparative results are generated against the existing method. Here figure 2 is showing the comparative results in terms of communication throughput.

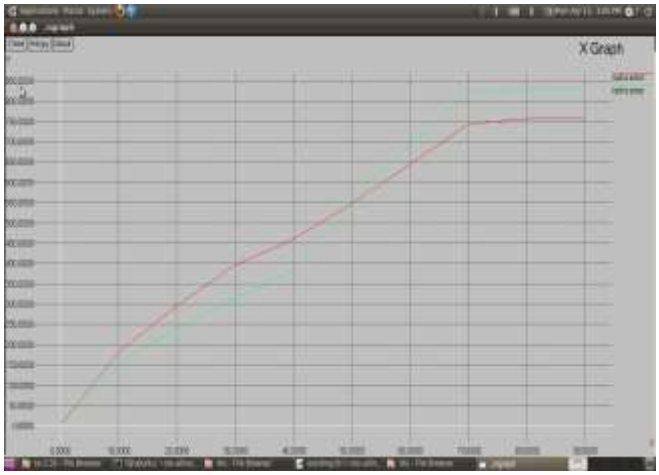


Figure 2 : Packet Transmission (Existing Vs. Proposed)

Here figure 2 is showing the comparative observation in terms of packet transmission analysis. Here green line is showing the communication results of presented approach and red line is showing the results of existing approach. The figure shows that at the earlier stage, the packet transmission is lesser in this work. But as the algorithmic implementation is performed, the work has improved the packet communication. Another parameter considered here is communication loss shown here in figure 3.

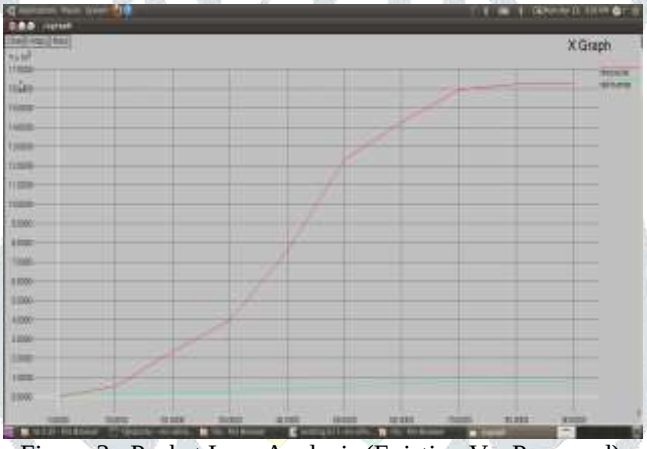


Figure 3 : Packet Loss Analysis (Existing Vs. Proposed)

Here figure 3 is showing the comparative results in terms of packet loss. The figure shows that the communication loss in case of proposed approach is very low. It shows that the method has improved the overall communication and reduced the communication failure. Third parameter taken here is communication delay shown here in figure 4.

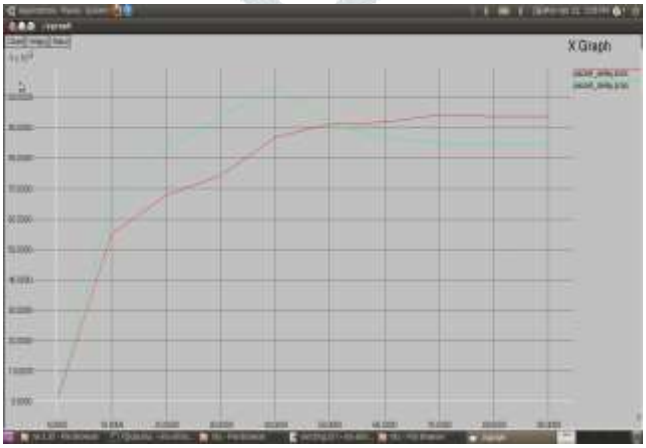


Figure 4 : Packet Delay Analysis (Existing Vs. Proposed)

Here figure 4 is showing the comparative observation in terms of communication delay. The results shows that at the earlier phase, the communication delay in case of proposed approach is higher, but later on after algorithmic implementation. The communication delay is reduced and overall network optimization is achieved.

## V. CONCLUSION

In this present work, an optimized weighted and probabilistic model is defined to identify the man-in-middle attack to provide the safe communication over the network. At the earlier stage, the session specific node analysis is defined at multiple communication vectors. These vectors are combined in weighted method to identify the safe and reliable nodes. In final stage of this model, the probabilistic method is applied to generate the safe communication path over the network. The simulation results show that the proposed method reduced the communication delay and loss.

## REFERENCES


[1] V. Kumar, S. Chakraborty, F. A. Barbhuiya and S. Nandi, "Detection of stealth Man-in-the-Middle attack in wireless LAN," Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, Solan, 2012, pp. 290-295.

[2] S. Sandhya and K. A. S. Devi, "Contention for Man-in-the-Middle Attacks in Bluetooth Networks," Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, Mathura, 2012, pp. 700-703.

[3] Huan-Rong Tang, Rou-Ling Sun and Wei-Qiang Kong, "Wireless Intrusion Detection for defending against TCP SYN flooding attack and man-in-the-middle attack," 2009 International Conference on Machine Learning and Cybernetics, Baoding, 2009, pp. 1464-1470.

[4] Z. Chen, S. Guo, R. Duan and S. Wang, "Security Analysis on Mutual Authentication against Man-in-the-Middle Attack," 2009 First International Conference on Information Science and Engineering, Nanjing, 2009, pp. 1855-1858.

[5] K. Bicakci, D. Unal, N. Ascioglu and O. Adalier, "Mobile Authentication Secure against Man-in-the-Middle Attacks," Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on, Oxford, 2014, pp. 273-276.

[6] Z. Chen, S. Guo, K. Zheng and Y. Yang, "Modeling of Man-in-the-Middle Attack in the Wireless Networks," 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, 2007, pp. 2255-2258.

[7] U. Meyer and S. Wetzel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks," Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on, 2004, pp. 2876-2883 Vol.4.

[8] L. Zhang, W. Jia, S. Wen and D. Yao, "A Man-in-the-Middle Attack on 3G-WLAN Interworking," Communications and Mobile Computing (CMC), 2010 International Conference on, Shenzhen, 2010, pp. 121-125.

[9] K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures," in IEEE Transactions on Wireless Communications, vol. 9, no. 1, pp. 384-392, January 2010.

[10] K. M. J. Haataja and K. Hypponen, "Man-In-The-Middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures," Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on, St Julians, 2008, pp. 1096-1102.

[11] F. Fayyaz and H. Rasheed, "Using JPCAP to Prevent Man-in-the-Middle Attacks in a Local Area Network Environment," in IEEE Potentials, vol. 31, no. 4, pp. 35-37, July-Aug. 2012.

[12] L. Galluccio, G. Morabito and M. Catania, "Facing man-in-the-middle and route diversion attacks in energy-limited RFID systems based on mobile readers," Ad Hoc Networking Workshop (Med-Hoc-Net), 2011 The 10th IFIP Annual Mediterranean, Favignana Island, Sicily, 2011, pp. 58-64.

[13] M. Agarwal, S. Biswas and S. Nandi, "Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks," in IEEE Communications Letters, vol. 19, no. 4, pp. 581-584, April 2015.

[14] G. Nath Nayak and S. Ghosh Samaddar, "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, Chengdu, 2010, pp. 491-495.

[15] S. Y. Nam, D. Kim and J. Kim, "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks," in IEEE Communications Letters, vol. 14, no. 2, pp. 187-189, February 2010.