International Journal of Advanced Trends in Computer Applications
www.ijatca.com

ENHANCED SECURITY WITH DETECTION AND CORRECTION OF MALICIOUS NODE IN WIRELESS AD HOC NETWORKS USING PSO WITH MD5

[1]Jyoti Bains, [2]Er. Bhupinder Singh
[1,2]Computer Science Department,
Indo Global College of Engineering, PTU

Abstract: *Wireless ad hoc networks are accumulation of wireless nodes which communicate precisely above prevailing wireless channel. The nodes are rigged with the wireless transceiver. In ad hoc network a node can disseminate only with nodes in its area, such node can communicate with other nodes, but a routing algorithm is imperative. Link error and malicious packet dropping are two means by which packet loss can occur. It is paramount for detect and encounters whether the losses are by cause of link errors only, or is by virtue of both link error and malicious packet drop. Absolute interest is in the insider incursion case where such malicious nodes abandon and decline packets selectively to deteriorate the network performance. Bitmap for transmission of packets of each node is obtained. By using the bitmap, correlation can be obtained between the lost packets and from this correlation, malicious node can be identified. For correlation of lost packets HLA based mechanism is used to verify the malicious node which is responsible for packet dropping. PSO technique is used for securing data transmission. This is symmetric encryption algorithm. In this encryption key is public whereas the decryption key which is kept secret. MD5 algorithm is used to maintain and assure the accuracy and consistency of data, integrity of data. Random numbers are sending during iteration as an encrypted value so as to enhance security. In case of unauthorized access the data is not misplaced or corrupted due to this property of sending random numbers. After finding the malicious node and error that is whether it is due to link error or the combination of malicious node and link error substitute of malicious node can also be attained via PSO algorithm.*

Keywords: *Homomorphic Linear Authenticator, Particle Swarm Optimization, Message Digest Algorithm.*

I. INTRODUCTION

Wireless ad hoc networks are accumulation of wireless nodes which communicate precisely above prevailing wireless channel. The nodes are rigged with the wireless transceiver. Every node doesn't alone perform the performance of an end system, although also pretends as a router, which transmits packets to covet nodes. In a multi–hop wireless network, nodes collaborate in relaying/routing traffic. An adversary can exploit this cooperative nature to launch attacks. Once being included in a route, the attacker starts dropping packets. In the most severe form , the malicious node simply hinder forwarding every packet acquired from upstream nodes, completely disrupting the path between the source and the destination . The ad hoc are anticipated to do appointment tasks that the infrastructure can't perform. Ad hoc networks are generally used by rescue mission team, military, taxi driver, many more. Here, in the ad hoc network a node can communicate only with nodes in its area, such node can communicate with other nodes, but a routing algorithm is vital. In the case of computer networks, the ad hoc networks are a wireless network but without infrastructure, they also known as spontaneous network. Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such as "always on" attack has its disadvantages. First, the continuous presence of extremely high packet loss rate at the malicious node makes this type of attack easy to be detected. Second, once being detected, these attacks are easy to mitigate. A malicious node that is a part of the route can venture its knowledge of the network protocol and the communication

context to dispatch an insider attack- an attack that is infrequent, but can achieve the same performance deterioration effect as a persistent attack at a much lower risk of being detected.

PSO

This algorithm is described by Eberhart, Shi and Kennedy named Particle Swarm Optimization in 1995. This scheme is applicable for optimizing an issue frequently arduous to embellish a solution with approbation to a given quality measure. Particle swarm optimization algorithm was pursued to perform optimization and it was the algorithm first premeditated to imitate the social behaviour of an organism for example bird. PSO is an optimization algorithm that is partly erratic, noisy and in there occurs the stagnation point, that hinders the communication. In PSO, the swarm consists of particles which move around the solution space of the issue. These particles search for the optimal solution of the problem in the predefined solution extent till the convergence is acquired.

For binary discrete search space, Kennedy and Eberhart have adapted the PSO to search in binary spaces by applying a sigmoid transformation to the velocity component in the equation to squash the velocities into a range [0,1] and force the component values of the positions of the particles to be 0's or 1's. The sigmoid expression is given by

$$\text{sigmoid}(p_{id}^k) = \frac{1}{1 - e^{-v_{id}^k}}$$

$$\text{where} \qquad p_{id}^k = \begin{cases} 1, \text{if rand}(\,) < \text{sigmoid}(p_{id}^k) \\ 0, \text{otherwise} \end{cases}$$

Feature selection using binary PSO:

Feature selection is performed to reduce the dimensionality of facial image so that the features extracted are as representative as possible. Method employed here is Binary PSO. Consider a database of L subjects or classes, each class W1, W2, W3… WL with N1, N2, N3,…NL number of samples. Let M1, M2, M3... ML is the individual class mean and M0 be mean of feature vector. Fitness function is defined so as to increase the class separation equation. By minimizing the fitness function, class separation is increased. For iteration the most important features are selected. Binary value of 1 of its position implies that the feature is selected as a distinguishing feature for the succeeding iterations and if the position value is 0 the feature is not selected. The expressions for class, individual mean and mean of feature of feature vector are shown below.

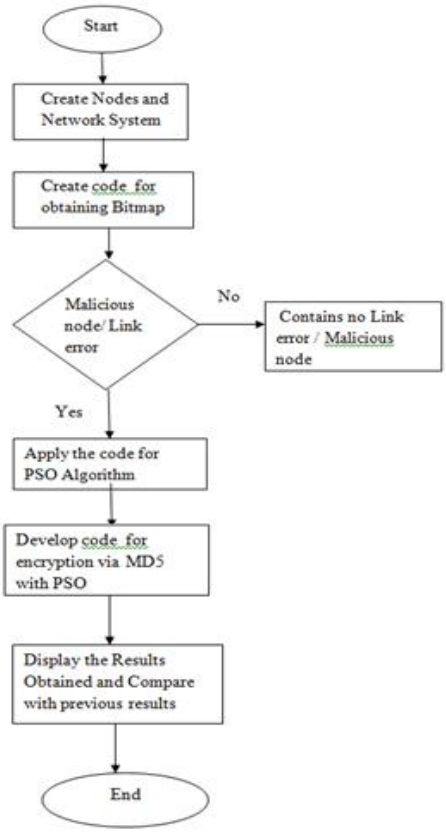
$$W_j^{(i)}, \text{ for } j = 1, 2, \ldots, N_i$$

$$M_i = \frac{1}{N_i} \sum_{j=1}^{N_i} W_j^{(i)}, \quad \text{for} \quad i = 1, 2, \ldots, L$$

$$M_0 = \frac{1}{N} \sum_{i=1}^{L} N_i \times M_i$$

MD5

The MD5 message-digest algorithm is a extensively used cryptographic hash function producing a 128-bit (16-byte) hash value, typically declared in text format as a 32 digit hexadecimal number. MD5 has been employed in a wide variety of cryptographic applications, and is also generally used to authenticate data integrity. MD5 digests have been extensively used in the software world to provide some affirmation that a transferred file has arrived unviolated. MD5 consists of 64 of these operations, arranged in four rounds of 16 operations. *F* is a nonlinear function; one function is used in each round. *Mi* signifies a 32-bit block the message input, and *Ki* signifies a 32-bit constant, different for each operation. *s* signifies a left bit rotation by *s* places; *s* varies for each operation.



Flowchart of the Proposed System

II. OBJECTIVE

There are mainly five objectives that are mentioned in this paper. First is to study the detection of malicious node. Second is to observe the packet loss sequence in network. Third is to determine whether the losses are due to Link error or by the combined effect of link error and malicious node. Fourth is to analyze and design the performance of Ad Hoc network using PSO and HLA algorithms and last is to optimize the encryption of data authentication of malicious node and causes of packet losses.

III.METHODOLOGY

This paper will include the development of a code for the GUI and a code for the creation of the various wireless nodes (Source node, central node and destination node) in the editor window of the MATLAB. Further at the time, when the packet is transmitted from source node to destination node, the development of a code will be done for obtaining the bitmap for each node. Development of a code for authenticating the malicious node and for maintaining the integrity, HLA algorithm will be used. After that encryption and decryption of the information will be done to secure data transmission and coding will be done for the PSO algorithm. Lastly the development of the code will be done for the calculation of the performances and the implementation comparisons.

IV. SIMULATION RESULT AND DISCUSSION

In this Paper, the performance of miss Detection probability and Overall detection-error probability compared with each other. The results of all the intermediate steps of the proposed methods are highlighted Implementation is done on MATLAB. Experimental results of intermediate steps show the efficiency of the proposed approach.

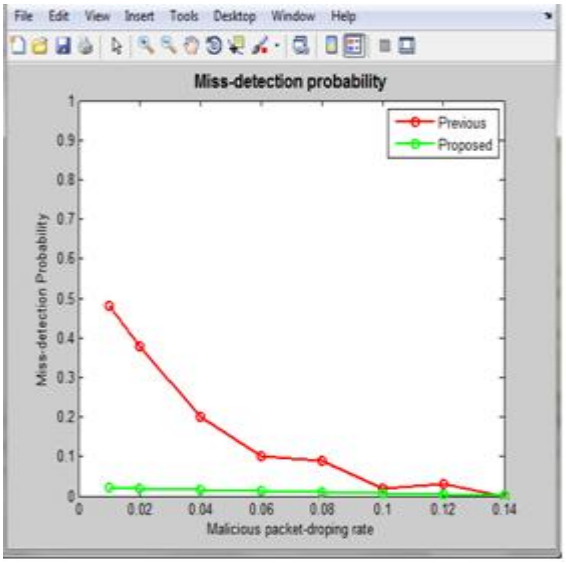


Figure 1: A comparison graph for Miss-detection probability

Here, we compare the miss-detection probability with the previous proposed system. And we get better result than previous result. Simulation result of Miss-detection probability is found on the basis of malicious packet-dropping rate.

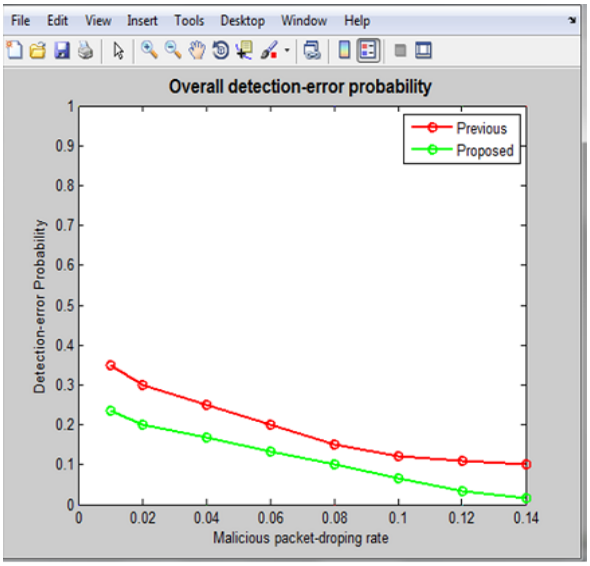


Figure 2: A comparison graph for Overall detection-error probability

Here, we compare the Overall detection-error probability with the previous proposed system. And we get better result than previous result. Simulation result of Overall detection-error probability is found on the basis of malicious packet-dropping rate.

V. CONCLUSION

In this paper we present results compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting

malicious drops. Such improvement is especially visible when the number of maliciously dropped packets is calculate the correlation between lost packets, it is critical to acquire truthful packet loss information at individual nodes. We developed the PSO Algorithm with MD5 technique which achieves better accuracy result in case of packet loss in wireless ad hoc network. In case of selective packet dropping attacks, conventional methods are not able to provide satisfactory result. For the correct calculation of correlation between lost packets, it is important to get truthful information about packet loss. So, PSO based auditing mechanism is developed that provides the truthfulness for the packet loss information provided by the intermediate nodes in the network.

REFERENCES

[1]. Tao Shu and Marwan Krunz "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks" in Wireless AdHoc Networks", June 2014.

[2]. Amutha.S, Balasubramanian.K, "Secure Implementation of Routing Protocols for Wireless Ad hoc Networks" pp. 960-965, Feb 2013.

[3]. Shu.T, Krunz.M, and Liu.S, "Secure data collection in wireless sensor networks using randomized dispersive routes". Vol. 9, no. 7, pp. 941–954, Mar 2010.

[4]. Proano.A and Lazos.L "Packet-hiding methods for preventing selective jamming attacks" Dependable and Secure Computing., vol. 9, no. 1, pp. 101–114, Aug 2012.

[5]. Noble George and Sujitha M "Truthful detection of packet dropping attack in MANET" International Journal of Advanced Research in Computer and Communication Engineering, vol. 4 issue 7, 2015.

[6]. Bobby Sharma Kakoty, S. M. Hazarika and N. Sarma "NAODV- Distributed Packet Dropping Attack Detection in MANETs"International Journal of Computer Applications (0975-8887), vol. 83- no. 11, 2013.

[7]. Dr. C. Kumar Charliepaul and K. Megala Devi "Secure routing and Attack detection in wireless AD HOC Network" International Journal on Engineering Technologies and Sciences, vol. 1 issue 6, 2014.

[8]. Wang.C, Wang.Q, Ren.K, and Lou.W. "Privacy-preserving public auditing for data storage security in cloud computing", IEEE INFOCOM, Mar. 2010.

[9]. B. Sun, Y. Guan, J. Chen and U. W. Pooch, Detecting black- hole attack in mobile ad hoc networks, In Proc. 5th European Personal Mobile Communications Conference, Glasgow, UK, April 2003.

[10]. Munir S.A., Biao Ren, Weiwei Jiao, Bin Wang Dongliang Xie and Jian Ma, "Mobile Wireless Sensor Network: Architecture and Enabling Technologies for Ubiquitous Computing", Advanced Information Networking and Applications Workshops, vol.2, pp.113-120, 21-23 May 2007.