Biomedical Research 2016; Special Issue: S174-S177 *ISSN 0970-938X*
www.biomedres.info

An investigation on selective jamming attacks based on swarm intelligence optimized multi-metric packet hiding method.

Ramesh Kumar M[1*], Sakthivel S[2]

[1]Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, Tamilnadu, India

[2]Department of Computer Science and Engineering, Sona College of Technology, Salem, Tamilnadu, India

Abstract

Wireless network is a group of computer network devices using wireless communication. There are many types of jamming attacks affecting in wireless communication. In order to avoid the jamming attacks in the flow of network communication, the network security helps us to manage the uninterrupted solution to wireless communication. By using swarm intelligence, can provide the collaborative deductive solution to the different jamming attacks in wireless communication. This investigation provides on security issues of wireless sensor networks requirements and challenges for Wireless Sensor Networks (WSN). Wireless sensor networks provide ordered and reliable observation of few features of physical phenomena which are otherwise very difficult to scrutinize and also the instigation of right actions based on collective information from wireless sensor network nodes. The application of swarm intelligence optimization helps on several network performance and social applications such as target tracking, disaster management, field inspection, ecological and habitation monitoring, healthiness application, residence automation and traffic management has been pointed out.

Keywords: Selective jamming attacks, Swarm intelligence.

Accepted on August 30, 2016

Introduction

Swarm intelligence works us a distributive system of integrating independent forces. This will continue to grow; security becomes important in recent times. Jamming attack has to deduct by using these techniques like swarm intelligence, cryptographic and passing random packets methods. It offers distributive and self centered system for adaptation of network security and generating a route for multipath access in safe mode. The wireless sensor network performs in network processing to reduce large amount of raw information in to needed comprehensive information.

The process of protecting packet is very critical and cannot use directly in the network process. This is a challenging area, where swarm intelligence technique gives the security solutions from the risk of unauthorized usages in network communication. Denial of services helps us to identify the delayed sending packet those affected as unsecured packets in network communication.

This paper helps to find out the solutions for jamming attacks using multi-metric packet hiding method, this will help the network administrator to manage it in efficient manner. Multi metric optimization provides multi objective solution having different trade-offs between the network security nodes.

Overcrowding attacks is highly difficult to preventing wireless transmission. This attack is working as continuous transmission of high power interference signals. A multi metric method is one of a technique which helps us an anti-overcrowding attack. To deduct this attack in wireless network we can use metrics like packet release ratio, signal strength and pulse intensity. To measure the overcrowding attack uses the threshold value to determine the range of signal strength of wireless network. Another technique is called as all-or-nothing protocol transformation method. This helps us to transform the encrypted data in a hide able manner for communicating our information in a secured way. This technique will also apply in cryptographic method.

Existing Research

While doing in the network communication the data has transferred from source to destination, during that time there is a possibility of hacking the packets. As per the previous literatures [1-14], if the packet is not reached the destination then only they check the status of the data packet. The channel hopping technique is used for checking the non-transferred packed in the wireless communication. If the packet is affected by the hackers the above technique will help to re-transmit the packet by selecting the new path and technique in the network channels. The current problems are, in swarm intelligence method is not hiding the location of network channels in frequency time. Optimal threshold value is not considered while generating random key.

Proposed Research

We use the swarm intelligence technique in multi-metric method for computing the jamming region for deduction purpose. Based on the threshold selection firefly algorithm calculation for signal strength parameters are identified. This algorithm helps us to monitor the brighter and attractive locations to select the optimal threshold in signal strength. To check the attack rates, this method helps to reduce the complexity of computation and unnecessary process of all nodes.

Another problem is communication overhead among all nodes in wireless communication. This can be reduced by using ant colony optimization on swarm intelligence. The forward and backward ant helps to reduces complexity on nodes channel information. By using channel hopping technique can use the sender and receiver information even away from the destination.

This proposed research helps us to reduce the selective jamming attacks both computation and communication overhead using swarm intelligence techniques.

We introduce simplified particle swarm optimization as an alternative of Ant colony Optimization, to increase the speed of collecting channel information. Particle based swarm to collect the channel information from all nodes and measures the packet sending ratio. The main problem to be implemented in the research work is as following as:

1. The multi metric method is used to detect the attacks during the data packet jamming. The multi metrics such as Packet Delivery Ratio (PDR), strength of the signal and band width are considered to finding the jamming attacks in the wireless networks. The average plus of jamming is computed and compare with the threshold value to detect the jamming attacks.
2. The firefly algorithm is used for the optimal threshold selection process. The all-or-nothing transformation method is used for packet hiding data in presented for mitigating the jamming attacks.
3. The work were carried out for evaluating the performance of the packet hiding method in the proposed Optimized Multi-Metric method and Packet Hiding method (OM3-PHM).
4. Based on the previous result to reduce the communication and computational overhead, The Swarm Intelligence All or nothing transformation (SIAONT) and optimized multi metric method for packet hiding method combined together. This combined method is known as Swarm Intelligence Optimized Multi Metric Method and Packet Hiding Method (SIOM3-PHM).

Investigation of Jamming Attack

This work introduces Optimized Multi-Metric method and Packet Hiding method (OM3-PHM) for detecting and preventing the jamming attacks in the wireless networks. This method uses the multiple metrics for detecting the jamming attacks with the support of swarm intelligence. The metrics include Packet Delivery Ratio (PDR), signal strength variation and pulse width. The packet delivery ratio in the designation is measured by the given sample of time frame. The difference in the signal strength and pulse width is the model parameters of the jamming attacks. The packet jamming detection is detected by measuring the average jamming pulse for the frame of N templates. The occurrence of jammer is determined by comparing the jamming pulse with the given threshold value. The firefly algorithm is used to compute the optimal threshold value. In the firefly algorithm, the objective function of an optimization problem is according to the light intensity. The fireflies move towards brighter and attractive positions for acquiring the optimal solutions in the packet hiding. The entire fireflies are described by their light intensity related with the objective function. Every firefly is altering the position in an iterative manner. By using this method, the jamming attack is detected in an effective manner.

Then, mitigating the jamming attack in the wireless network all-or-nothing transformation method is presented. All-or-nothing Transformation is a new solution that introduces a modest communication and computation overhead. This transformation is basically proposed by Rivest to reduce the brute force attacks against block encryption algorithms. A new mode of encryption is called as all-or-nothing encryption method. The main idea of this concept is to decrypt the whole cipher text before one can determine even one message block.

Swarm intelligence optimized multi-metric method

In this section, the swarm intelligence multi-metrics are measured for detecting the jamming regions in the wireless sensor networks. This multi-metric method considers the PDR (Packet Delivery Ratio) and signal strength variation as the detection parameters.

PDR is defined as the ratio to find the numbers of nodes received perfectly to the number of nodes sent in wireless networks.

Signal strength is measured by the power of signal at the receiver end. Signal strength is considered as the detection parameter in a node. Two methods are used to describe the variation in the signal strength. They are the average value of signal strength in the time frame and the spectral discrimination technique.

The pulse width is measured in time of the packets which is taken in microseconds. The PDR is measured by

PDR= (Number of packets correctly received)/(Number of packets sent) → (1)

The Equation 1 is measured the PDR in the given sample time frame. Then, the PDR value is compared with the PDR threshold value PDRthr. If the measured PDR is less than the PDRthr value, variable signal strength is measured for the jamming attacks.

The Signal strength variation is measured by

$\Delta S=SS_{observed}-SS_{network} \rightarrow (2)$

In the Equation 2, $SS_{network}$ represents the strength of signal during training session without jamming attacks and $SS_{observed}$ denotes the signal strength evaluated when the wireless network is affected by the jamming attack. If the signal strength is less than the SSthr the jamming signal is detected. Based on the PDR and signal strength, the jamming pulse is detected.

The jamming pulse performs as a high-power Gaussian noise that can emerge many times in the channel. To evaluate the channel, N samples of channel's received energy s (t) are gathered. The gathered samples form a big window of samples like s (k), s (k-1),.. s (k-N+1) taken at the consecutive smaller sampling time windows. The jamming attack is detected by using the equation,

$$T_{(k)} = \left(\frac{\sum_{j=k-N+1}^{k} (s(j)^2)}{N} \right) \rightarrow (3)$$

In the Equation 3, $T_{(k)}$ denotes the average jamming pulse measured in the window of N samples. In order to determine the jammer attack in the wireless network $T_{(k)}$ is compared with the threshold value δ.

The firefly algorithm optimal threshold selection

The optimal value of the threshold is selected. For optimal threshold selection, the firefly algorithm is presented. The firefly algorithm is used to find the optimal solution by considering the objective function of a given optimization problem. The objective function for a given optimization problem is depends on the light intensity. This objective function is used to move the fireflies towards brighter and more attractive locations for acquiring the optimal solutions. The entire fireflies are described by the light intensity with the related objective function. Every firefly is changed its position iteratively to reach the best solution.

In this work, firstly the population of fireflies (Threshold values) is initialized. There are two significant points in the firefly algorithm. The variation in the light intensity and formulation of the attractiveness are the two significant points. The attractiveness is decided by the brightness of the fireflies in which the objective function is connected. Also, the objective function is used to compute the brightness I of the firefly in a particular position. The objective function is to reduce the False Error Rate (FER) in the jamming attack detection for the wireless networks.

I (x) =Minimum (FER) → (4)

Equation 4 gives the intensity of the fireflies in the wireless network.

The attractiveness function of the firefly is established by the Equation 5

$$\beta(r) = \beta_0 . ew^{-\gamma . r^2} \rightarrow (5)$$

Equation 5 gives the attractiveness of the firefly. In this equation, β_0 represents the attractiveness value of the firefly at r=0. γ denotes the media light absorption coefficient. The computation of the distance between the two fireflies i and j at the positions x_i and x_j is denoted as follows:

$$r_{ij} = \left\| X_i - X_j \right\| = \sqrt{\sum_{k=1}^{d} \left(X_{i,k} - X_{j,k} \right)^2} \rightarrow (6)$$

Equation 6 denotes the distance between the two fireflies. In this equation, $X_{i,k}$ represents the k^{th} element of the spatial coordinates X_i in the i^{th} firefly and d denotes the number of dimensions. The movement of the firefly i is represented as:

$$x_i = x_i + \beta_0 * \exp\left(-\gamma r_{ij}^2\right) * \left(x_j - x_i\right) + \alpha * \left(rand - \frac{1}{2}\right) \rightarrow (7)$$

In the Equation 7 the movement of the firefly is decided if the intensity value of the firefly is high. In this equation, the first term denotes the present position of the firefly I, the attractiveness of the firefly is represented in the second term and last term represents the movement of the firefly if there is no any brighter firefly. In some of the cases, α (0, 1) and β_0=1. The light absorption coefficient differs from 0.1 to 10.

Prevention of jamming attack using swarm intelligence optimized multi metric method

A new solution is presented in this method called Swarm Intelligence optimized Multi Metric Method (SIM3) for packet hiding to mitigate the jamming attacks in wireless networks. By using this method, there is less communication and computation overhead. This method utilized as a entire invertible hiding of text in pre-processing step to a plaintext before it is provided to the common block encryption method and send the acknowledge to the sender.

A original message m= $\{m_1, \ldots m_x\}$ is transformed into the sequence of pseudo messages $m'= \{m'_1, \ldots m'_x\}$ by using All-Or-Nothing (AONT) method. In the AONT process, if a plaintext is pre-processed before the encryption process, the entire cipher text is recovered in order to acquire the plaintext. Consequently, the brute force attacks are sluggish by a factor that is equivalent to the number of cipher text blocks without makes changes in the secret key size the receiver send back to the acknowledge to the sender.

By using the SIOM3 method, the packets are pre-processed before the transmission starts but it is in unencrypted format. The jammer cannot do the packet classification process until the entire pseudo-messages equivalent to the original packet message has been recovered and the inverse transformation has been used to recover the message. The packet m is divided into a set of input blocks m= $\{m_1, \ldots m_x\}$ in which used as an input for the AONT method f: $\{F_u\}^x \rightarrow \{F_u\}^{x'}$. In this equation, F_u denotes the alphabet of blocks m_i and x' denotes the number of pseudo-messages with $x' \geq x$. The set of pseudo-messages $m'= \{m'_1, \ldots m'_x\}$ is transmitted in the wireless medium. In the receiver side, the inverse transformation is used f^1 used after

all x' pseudo-messages are received in order to acquire the original messages.

In this packet hiding method, the forward ant and backward ant are used to collect channel information. In this channel information, the Packet Delivery Ratio (PDR) and variation in signal strength are determined. If any variation occurs, it can be compare with the threshold value. In this method prevent the jamming and attacks and avoid the communication and computation overhead.

False error rate

False error rate is defined as to detect the node as a jammer node in the wireless network without the presence of a jammer.

The false error rate comparison is used for the existing and proposed system. In the X-axis number of nodes is taken. In the Y-axis false error rate is taken. In the existing method, All-Or-Nothing Transformation (AONT) method is used for mitigating the jamming attacks. In the proposed method, SIOM3-PHM method is presented for detecting and mitigating the jamming attacks in the wireless networks. The proposed system is less false error rate in the proposed system.

Conclusion

This research is to conclude that detection and prevention of selective jamming attacks can be easily accomplishing using swarm intelligence optimized multi-metric packet hiding methods. This research achieves high throughput, increased packet delivery ratio and very less false error rate. This research establishes an effective packet hiding method while transmitting the data in wireless network with other prevention methods. The future work is further extended to deduction and prevention of attacks through spoofing, snooping, sniffing and fork bombs etc. in network security. This extension move towards on transportation network design problem to control traffic problem and find the optimal solution.

References

1. Lakshmi GJ, Babu S, Rao BL, Mohan P, Kumar BS. Jamming attacks prevention in wireless sensor networks using secure packet hiding method. Int J Adv Res Comp Comm Eng 2013; 2: 3429-3433.
2. Surya S, Swathigavaishnave D, Kanimozhi T. Swarm-based intelligent technique to prevent selective jamming attacks for dynamic topology. Int J Adv Res Comp Comm Eng 2014; 3: 8707-8710.
3. Periyanayagi S, Sumathy V. A swarm based defence technique for jamming attacks in wireless sensor networks. Int J Comp Theory Eng 2011; 3: 816.
4. Proano A, Lazos L. Packet-hiding methods for preventing selective jamming attacks. IEEE Trans Dep Sec Comp 2012; 9: 101-114.
5. Simon MK, Omura JK, Scholtz RA, Levitt BK. Spread spectrum communications handbook. McGraw-Hill 2001.
6. Wilhelm M, Martinovic I, Schmitt J, Lenders V. Reactive jamming in wireless networks: How realistic is the threat. Proc ACM Conf Wireless Netw Secur 2011.
7. Thuente D, Acharya M. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. Proc IEEE Military Comm Conf 2006.
8. Brown TX, James JE, Sethi A. Jamming and sensing of encrypted wireless ad hoc networks. Proc ACM Intl Symp Mobile Ad Hoc Netw Comp 2006; 120-130.
9. Dempsey T, Sahin G, Morton Y, Hopper C. Intelligent sensing and classification in ad hoc networks: A case study. IEEE Aerosp Electr Sys Magaz 2009; 24: 23-30.
10. Liu X, Noubir G, Sundaram R. Spread: foiling smart jammers using multi-layer agility. Proc IEEE INFOCOM 2007; 2536-2540.
11. Greenstein B, Mccoy D, Pang J, Kohno T, Seshan S, Wetherall D. Improving wireless privacy with an identifier-free link layer protocol. Proc Intl Conf Mobile Sys App Services 2008.
12. Lazos L, Liu S, Krunz M. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. Proc ACM Conf Wireless Netw Secur 2009; 169-180.
13. Strasser M, Popper C, Capkun S. Efficient uncoordinated fhss anti-jamming communication. Proc ACM Intl Symp Mobile Ad Hoc Netw Comp 2009; 207-218.
14. Alejandro P, Loukas L. Packet-hiding methods for preventing selective jamming attacks. IEEE Trans Depend Secur Comp 2012; 9: 101-114.

*Correspondence to

Ramesh Kumar M

Department of Computer Science and Engineering

Dhirajlal Gandhi College of Technology

India