P. Narasimha Rao et al, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 7, July- 2014, pg. 06-11 **ISSN: 2321-8363**

# Secure Packet Transmission for Preventing Selective Jamming Attacks

**P. Narasimha Rao, B. Siva Rama Krishna, Dr. Sai Satyanarayana Reddy**
[1]M.Tech, CSE, LBRCE, Mylavaram, India, narasimhacm079@gmail.com
[2]Assistant Professor, CSE, LBRCE, Mylavaram, India, sivaram6115@gmail.com
[3] Professor, CSE, LBRCE, Mylavaram, India, saisn90@gmail.com

***ABSTRACT:*** ***Wireless networks are susceptible to numerous securities threats due to the open nature of the wireless medium. Anyone with a transceiver can eavesdrop on ongoing transmissions, inject Spurious messages, or block the transmission of legitimate ones. One of the fundamental ways for degrading the network Performance is by jamming wireless transmissions. These Jamming attacks can be used for launching Denial-of-Service attacks on wireless networks. Jamming has been considered as external attack model, but if the attack is internal it cannot be solved by using methods such as spread spectrum methods. In case of internal attacks, the adversary launches jamming attacks in which it targets highly important packets. We illustrate the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol. A swarm based vulnerable prevention mechanism based on swarm intelligence is proposed against jamming attacks in wsn. Swarm intelligence algorithm is good in adapting according to change in network topology and traffic. Another method named channel surfing methods using attracting nodes to defend against selective jamming/dropping attacks is also proposed for enhanced security.***

## 1. INTRODUCTION

Wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium. Anyone with a transceiver can eavesdrop on ongoing transmissions, inject spurious messages, or block the transmission of legitimate ones. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions [9], [11], In the simplest form of jamming, the adversary corrupts transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers. For an adversary agnostic to the implementation details of the network, a typical jamming strategy is the continuous emission of high-power interference signals such as continuous wave tones, or FM modulated noise. However, adopting an "always-on" jamming strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of high interference levels makes this type of jamming easy to detect. Third, these attacks are easy to mitigate either by spread spectrum communications, spatial retreats, or localization and removal of the jamming nodes. In this paper, I consider a sophisticated adversary model in which the adversary is aware of the implementation details of the network protocols. By exploiting this knowledge, the adversary launches *selective jamming attacks* in which it targets specific packets of "high" importance. For example, jamming of TCP acknowledgments (ACKs) can severely degrade the throughput of a TCP connection due to the congestion control mechanism of the TCP protocol [3]. Compared to continuous jamming, the adversary is active for a short period of time, thus expending orders of magnitude less energy. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet, for example, by decoding the frame control field of a MAC-layer frame. We are interested in developing *resource efficient* methods for preventing real-time packet classification and hence, mitigating selective jamming. Our contributions are summarized below. We investigate the feasibility of real-time packet classification for launching selective jamming attacks [11], [16], [17]. We consider a sophisticated adversary who exploits his

 

knowledge on network protocols along with secrets extracted from compromised nodes to maximize the impact of his attack. To mitigate selective jamming, we combine cryptographic mechanisms such as commitment schemes, cryptographic puzzles, and all-in-one transformations, with physical-layer parameters. We further study the impact of various selective jamming strategies on the performance of the TCP protocol [6]. The remainder of the paper is organized as follows. Section II presents related work. In Section III, we describe the problem addressed, and state the system and adversarial model assumptions. In Section IV, we illustrate the feasibility of selective jamming attacks. In Section V, we develop methods for preventing selective jamming. Section VI, illustrates the impact of selective jamming on the performance of TCP.

## 2. RELATED WORK

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s. Recently, several alternative jamming strategies have been demonstrated. Xu et. Al [8]. categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected. Intelligent attacks which target the transmission of specific packets were presented in. Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer. Law et. al. considered selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were inferred from prior transmissions in other hops. However, in both , real-time packet classification was considered beyond the capabilities of the adversary. Selectivity was achieved via inference from the control messages already transmitted. Channel-selective jamming attacks were considered in . It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of magnitude. To protect control channel traffic, control information was replicated in multiple channels. The “locations” of the channels where control traffic was broadcasted at any given time, was cryptographically protected. In , we proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers. Finally, P¨opper et. al. proposed a frequency hopping anti-jamming technique that does not require the sharing of a secret hopping sequence, between the communicating parties.

## 3. SWARM INTELLIGENCE

An algorithm is selected based on the design constraint and the performance expected from the application. As each approach possesses trade off, the main criteria in selecting an algorithm is the time and probability of obtaining an optimal solution [5]. For example, an evolutionary algorithm may not always provide the global solution Swarm Intelligence, is an algorithm that models the collective behaviour of social insects, namely the ants, bees, birds, slime mould, etc. Ant system is one such evolution from the swarm intelligence forming an evolutionary algorithm with unique characteristics such as robustness, distributed problem solving, versatility and de-centralization approach. The ant system solves any complex convex optimization problem. It also adapts to the network with environmental changes. The agents in the system communicate interactively either directly or indirectly in a distributed problem- solving manner. The agents move towards the optimal solution and communicate directly by sharing knowledge with their neighbours the initial set of agents traverse through the nodes in a random manner, and once they reach their destinations, they deposit pheromone on trails as a means of communicating indirectly with the other ants. The amount of pheromone left by the previous ant agents increases the probability that the same route is taken during the current iteration. Other performance factors discussed in Section 3 also affect the probability of selecting a specific path or solution. Pheromone evaporation over time plays an important role in preventing suboptimal solutions from dominating in the beginning. In the system, the agents minimize energy and keep track of network requirements. As the ant moves from node to node, energy is lost through communication. The ant stops traversing a node once its energy is depleted. New paths are set up to avoid the node so that communication continues without the degraded sensor. These agents ensure that the optimal route to the destination using limited resources and also learning the network environment. Initially, the computational cost and time is high but this drops drastically once the agents learn the network and environment. A Tabu-list serves as memory tool listing the set of nodes that a single ant agent has visited. The ant’s goal is to visit nodes in the network depending on the number of hops assigned by the user. Thus traversing all the nodes and depleting all the energy at every node is avoided. In a given tour, a node

 

is never re-visited. The pheromones on all the paths are updated at the end of a tour. The pheromone deposition, tabu-list, and energy monitoring help this novel ant system (AS) to obtain an optimal solution and adapt it as nodes degrade.

## 4. ANTS IMPLEMENTATION

A swarm based defence method for jamming attacks in wireless sensor networks is proposed. Swarm intelligence algorithm is capable enough to adapt change in network topology and traffic [5]. The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The jammers remain on a single channel, changing to disrupt any fragment that may be transmitted in the pulse jamming method. Using swarm intelligence mechanism, the forward ants would unicast or broadcast at each node depending on the availability of the channel data for end of the channel.

## 5. DENIAL OF SERVICE IN WIRELESS NETWORK USING ANT SYSTEM

A Denial of Service (DoS) attack on a network is typically used by illegitimate users to reduce the capacity of the network. Similarly, when the sensor network is encountered by a Denial of Service (DoS) attack, it reduces both the functionality and the overall performance of the network. In crucial applications such as disaster relief, health monitoring etc., reduced performance due to DoS will only make the network unfit for the application. Hence, detecting DoS attacks and defending the network by taking the necessary countermeasures helps in maintaining or improving the performance of the application. Interception or compromise of the secure information by an enemy is an act that cannot be neglected. Hence, appropriate security measures need to be taken at every layer of a protocol design. Many attacks are caused by intruders who have seldom or complete knowledge of the protocol. There has been research on the different kinds of possible DoS attacks on sensor network. Wood et al in had summarized different DoS attack and its effect on the sensor network. Though no defence mechanism is proposed in this survey but different possibilities to reduce the attacks are given. In the physical layer, using spread spectrum is often used to reduce jammer attacks. This paper concludes that due to the limited resources code spread as used in mobile networks cannot be used in WSN. In mapping protocol for nodes that surround a jammer is proposed. Using this approach, the protocol creates awareness in the neighbouring nodes to detect a jamming attack using message diffusion. Also, in this paper single-channel wireless communication is assumed. It is simulated using GloMoSim simulator with different range of jamming attack and neighbouring nodes. The protocol was robust (message re-routed and only loses data in inactive nodes) to failure rates of 20-25% of mapping nodes from twelve neighbouring nodes within communication range. In sybil attack on a network and routing layer of WSN is analyzed. Here it is assumed that a sensor node communicates with its neighbours using half-duplex and single radio with various channels. The process of identifying Sybil attacks is based on radio resource testing. Legitimate neighbouring nodes are allotted a single channel for identity. This process of identifying a Sybil attack cannot function if the spectrum is jammed. Hence, would lead to a false identification of a Sybil attack in most of the previous work in DoS attack the transmission is either assumed secure or intruded only for injecting wrong data. One of the major disadvantage of any network is becoming non functional or unable to communicate. This is the most adverse attack a sensor network can encounter. This attack can account towards node's inability to communicate in spite of enough resources. In this paper, an evolutionary algorithm helps in maintaining the performance of the network by finding an alternative solution when a node is jammed by an intruder.

## 6. JAMMER ATTACKS AND ITS CHARACTERISTICS

A jammer is a device which can partially or entirely disrupt a node's signal, by increasing its power spectral density (PSD). Jammer can never re-produce a signal nor can it pretend like a receiver node. The parameters such as signal strength of a jammer, the location and the type influence the performance of the network and each jammer has different effect on the node. Using SS technique the data is spread across the frequency spectrum making the signal resilient to jamming, noise and eavesdropping. There are different types of SS such as Direct Sequence (DS), Frequency hopping (FH), Time hopping (TH) and hybrid [4]. There are both advantages and disadvantages associated with using SS in sensor networks. The advantages are 1.Ability to alleviate multi-path interference, 2.Jamming attacks reduced, and 3 less power spectral density. The disadvantages are, 1.Bandwidth

 

inefficiency, 2.Comples implementation, and 3. Computational cost. Bluetooth uses FHSS, which consumes more power as frequency hops needs to be synchronized. Whereas, Zigbeeuses IEEE802.15.4 standard where DSSS with CSMA-CA is used. Of late Zigbee is being considered as a wireless technology for wireless sensor networks as it consumes less power. Differentiating the attack from nature needs knowledge of the various attacks that can be caused by an illegitimate user since an attack can completely eliminate a coverage area, and in applications where network cannot be immediately updated, the network performance will be poor. Hence, study of different characteristics of an attack keeps the attack attempts minimal as knowledge of the types of jammer helps in taking the appropriate countermeasure. In this paper, its assumed that there are four different types of jammer, namely: single-tone jammer, multiple tone jammer, pulsed-noise jammer and ELINT

### 6.1 Single-Tone Jammer

A single-tone jammer's frequency lies within the specified bandwidth of the signal being jammed. It targets any narrowband communication. Since traditional wireless sensor network use narrowband technology this kind of jammer tries to continuously jam the node within specified bandwidth, which might result in a dead link and diminishes the node's coverage

### 6.2 Multiple-Tone Jammer

A jammer that can disrupt the signal of some or entire channel of a multiple channel receiver. This type of jamming leads to a complete node failure, if the entire channel is compromised. The only time the node can recover is when the jammer is turned off. Typically, an intruder plays it safe while jamming a node by occasionally turning off its radio. Thus, make the neighbouring node assume the node is not under attack but rather lost its energy and needs recuperation. Hence, detections of a jammed node is very important.

### 6.3 Pulsed-Noise Jammer

A pulsed-noise jammer is a wideband jamming, which behaves like a pulsed signal by turning on and off periodically. The primary goal of this jammer is to disrupt the spread spectrum communication by spreading the peak jamming power during the "on" time. Two types of pulsed-noise jammers are considered, namely, slowly switching and fast switching jammers.

### 6.4 ELINT

ELINT is typically a passive system that tries to break down or analyze radar or communicating TCF signals. They may be integrated. In the following section, mathematical formulation based on the different types of jamming is described with simulations

## 7. Vulnerable Channel Detection

If the data about channel is available, the ants randomly choose a hop. As the checked ants reaches the source, the data collected is checked which channel there is presence of adversary long time, and those channels are omitted. The swarm intelligence method which updates the sensor details more efficiently and successfully. In our proposed work, DEEJAM is combined with swarm method such that swarm's forward and checked ants scan through all the channels in a fast way and detects effectively the jamming activity by informing the legitimate node. Then legitimate node swaps the channel by avoiding the affected channel [11]. This will improve the detection of a jammer quickly with less complication.

 

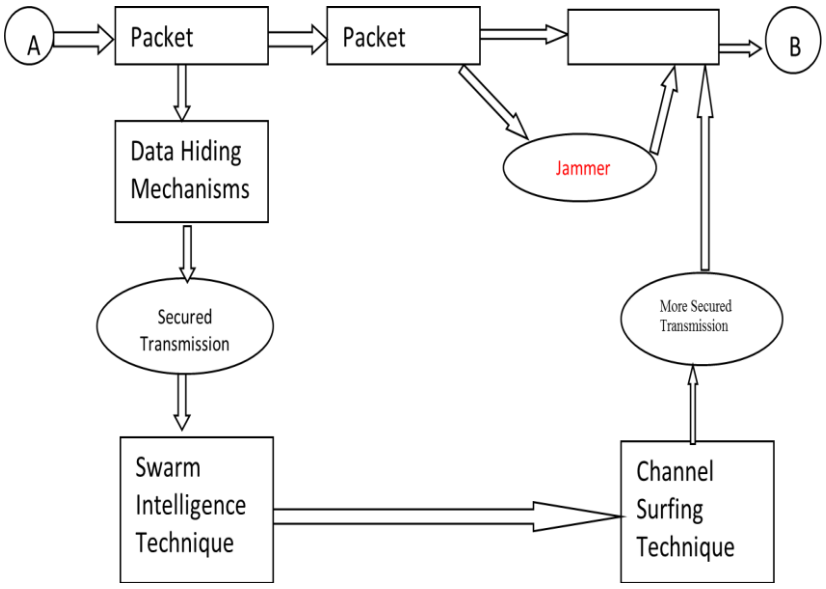


**Fig.1 System Architecture of Preventing Mechanism**

The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence. Using packet fragmentation method, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimiter). The last fragment contains a frame check sequence FCS for the entire payload. If the fragments are short, the adversary's jamming message does not start till the transmitter has finished transmitting and hopped to another channel. of these is a jamming based attack [4], [17]. This is because with the already existing network architecture, there is nothing that can be done to overcome a jamming attack. In this paper a pre-emptive detection policy using attracting nodes and a response mechanism based on the existing channel surfing algorithm is used to protect wireless nodes from a jammer. Attracting nodes generate duplicate communication at a frequency close to the actual frequency of operation, so that the true nodes can move to another frequency even before a jammer starts scanning that frequency.

## CONCLUSION

The selective jamming/dropping attacks can be launched by performing real-time packet classification at the physical layer. The proposed method investigates the impact of selective jamming/dropping on critical network functions and develops three methods that prevent classification of transmitted packets in real time. First the problem of real-time packet classification can be mapped to the hiding property of commitment methods and propose a packet-hiding method based on commitments. Second a packet-hiding method based on cryptographic puzzles. Finally All -or- Nothing Transformations that introduces a modest communication and computation overhead .A swarm based vulnerable prevention mechanism for jamming attacks in wireless sensor networks. Finally the swarm intelligence method which updates the sensor details more efficiently and successfully. This swarm based defence method for jamming attack is most effective. Using social insect metaphor for solving various problems is the main basis of swarm intelligence. Ants, bees, and termites are the insects which live in colonies. Every insect in colony have their own plans.

In our enhanced approach, swarm based vulnerable prevention mechanism for jamming attacks in wireless sensor networks. Swarm intelligence algorithm is capable enough to adapt change in network topology and traffic. The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The jammers remain on a single channel changing to disrupt any fragment that may be transmitted in the pulse jamming method. Using the swarm based vulnerable prevention method, the forward ants would unicast or broadcast at each node depending on the availability of the channel data for end of the channel. If the channel data is available, the ants randomly choose a hop.

 

As the checked ants reaches the source, the data collected is checked which channel there is presence of adversary long time, and those are omitted. At the same time the forward ants are sent through other channels which are not detected before for attacks. This method helps reduce the channel maintenance overhead. A pre-emptive detection policy using attracting nodes and a response mechanism based on the existing channel surfing algorithm is used to protect wireless nodes from a jammer. Attracting nodes generate duplicate communication at a frequency close to the actual frequency of operation, so that the real nodes can jump to another frequency even before a jammer starts scanning that frequency.

## REFERENCES

1. G. Sathish Kumar and V. Durgadevi " Providing Network Security by Preventing Selective Jamming Attack".pp 05-09 in Dec-2012.
2. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.
3. Rajani Muraleedharan and Lisa Osadciw, "Sensor Communication Networks Using Swarming Intelligence", IEEE Upstate New York Networking Workshop, Syracuse University, Syracuse, NY, October 10, 2003.
4. M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In Proceedings of WiSec, 2011..
5. Marco Doringo, "The Ant System: Optimization by a Colony of Cooperating Agents", IEEE Transactions on Systems, Man and Cybernetics-Part B, Vol-26, No. 1, Sept1996, pp 1-13.
6. P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 8(9):1221–1234, 2009.
7. K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009
8. H. Van Dyke Parunak, Sven Brueckner, " Ant like Missionaries and Cannibals : Synthetic Pheromones for Distributed Motion Control ", Proc of the 4th International Conference on Autonomous Agents(Agents 2000), pp. 467-
9. Alejandro Proano And Loukas Lazos January/February 2012 "Packet Hiding Methods for Preventing Selective jamming/dropping Attacks"IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (vol. 9 no. 1)
10. Lookas Lazos and Marwan Krunz February 2012 "Selective jamming/dropping/Dropping Insider Attacks in Wireless Mesh Networks" IEEE NETWORK Volume:25 Issue:4
11. Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang 2004"Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service" WiSe '04 Proceedings of the 3rd ACM workshop on Wireless security Pages 80 - 89 ACM New York, NY, USA
12. C. Po¨pper, M. Strasser, and S. Cˇ apkun. Jamming-resistant broadcast communication without shared keys. In *Proceedings of the USENIX Security Symposium*, 2009.
13. R. Rivest. All-or-nothing encryption and the package transform. *Lecture Notes in Computer Science*, pages 210–218, 1997.
14. M. Simon, J. Omura, R. Scholtz, and B. Levitt. *Spread spectrum communications handbook*. McGraw-Hill Companies, 1994.
15. D. Stinson. *Cryptography: theory and practice*. CRC press, 2006.
16. P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 8(9):1221–1234, 2009.
17. Alejandro Proano and Loukas Lazos "Packet-Hiding Methods for Preventing Selective Jamming Attacks". Presented at IEEE ICC 2010

 