International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Jamming Attacks Detection in Time-Critical Wireless Applications

Prajakta V. Pandhare[1], Jayant Adhikari[2]

[1]Tulsiramji Gaikwad-Patil College of Engineering & Technology, Mohgao Nagpur, India
[2]Tulsiramji Gaikwad-Patil College of Engineering & Technology, Mohgao Nagpur, India

Abstract: ***Most recently development of digital physical frameworks has grown tremendously; because of the fact that, the wireless networking applications has been drawing expansive interest of studies. The various attacks that are found in the wireless networks are described in this paper, and how these attacks can be detected and prevented in wireless applications. The main objective of this system is finding Jamming attack and the Replay attack. Because of the shared and open nature of wireless networks, the Jamming attacks occurs, which shows the radio obstruction in influencing the system ability. The previous methods are partially successful in detecting these types of attacks. But the real problem in the existing system is to detect and prevent jamming and replay attack. Thus, we provide a novel method to detect and prevent the jamming attacks by use of time limit. It also helps for detecting and preventing of Replay attack and blocking IP address of actual attacker in the network. Prevention is done by filtering the replay packet which is responsible for time critical network Jamming and Delay.***

Keywords: Jamming attack detection, wireless network, replay packet attack detection

1. Introduction

Wireless communications gives both adaptability and expense savings in deployment and maintenance contrasted with wire lined deployments. We gain simplicity of deployment, adaptability, and expense savings with wireless communications. Providing security and trustworthiness will turn into an issue of basic criticalness since wireless networks becoming popular. Regular difficulties connected with wireless communications are probabilistic channel behavior, inadvertent and controlled interference or unauthorized modification of the communications or eavesdropping, and jamming if not secured by authentication and encryption. A wireless correspondence system without obeying security protocols can be abused with a man-in-the-middle attack. This causes both loss of administration and loss of privacy.

Previous few studies have been focused on jamming-style attacks and the meaning of this type of attack stays indistinct. A typical supposition is that a jammer persistently radiates RF signals to fill a wireless channel, so honest to goodness traffic will be totally blocked. Then again, a more extensive scope of behaviors can be embraced by a jammer. The normal trademark for all jamming attacks is that their communications are not consistent with MAC protocols. Hence, a jammer can be characterized as an element who is attempting to interfere with the transmission and gathering of wireless communications. A jammer can achieve this objective by either keeping a genuine traffic source from conveying a bundle, or by keeping the gathering of honest to goodness packets. We focus mainly on jamming attack as they are easy to launch and difficult to detect. In [1], introduce new technique, message invalidation ratio to identify the impact of jamming attack.

A replay attack is a type of network attack in which a legitimate data transmission is vindictively or deceitfully rehashed or postponed. This is completed either by the originator or by an adversary who captures the data and retransmits it. The replay attacks can be summed up as: an attack on a security protocol utilizing replay of messages from an alternate context into the expected (or unique and expected) context, in this way tricking the honest participant(s) into supposing they have effectively finished the protocol run [2].

The development of today's wireless network like 3G/4G and Wi-Fi has as of now bring huge change and profit to individuals' life, for example, omnipresent wireless internet access. In the numerous application wireless network can be used the applications like cyber physical system, military application, etc. The main application of the wireless network is to transits the message or data from one place to another, while transmitting the message it is responsible for rising the attacks like jamming attack and replay packet attacks. Researchers focus is on generating the effective method for detection and prevention of this type of attack from the wireless sensor network.

2. Related Work

Li et al [3], have considered controllable jamming attacks that are not difficult to dispatch and hard to detect and stand up to, since they vary from brute force attacks. The jammer controls probability of jamming and transmission go to cause maximal harm to the network as far as adulterated communication links. They have especially helped; (i) determined the ideal assault and protection systems as answers for advancement issues that are confronted by the aggressor and the network individually by incorporating in the detailing vitality restrictions, (ii) for assault detection, gave an ideal detection test that determines choices focused around the measurable rate of brought about crashes, (iii) included in the definition assault detection and exchange of the assault warning message out of the jammed region.

M Strasser et al [4] address and depict the opposition to jamming/key establishment circular dependency issue:

Licensed Under Creative Commons Attribution CC BY

against jamming spread spectrum communication procedures depend on a shared (spreading) key and key establishment depends on a jamming-safe communication. As one answer for the tended to issue, they have proposed a plan called UFH (Uncoordinated Frequency Hopping) that empowers two nodes to execute a key establishment protocol in the vicinity of a jammer; the made key can then be utilized to help later coordinated frequency hopping communication. The UFH plan underpins the transmission of messages of subjective length in a jammed environment without depending on a shared secret key.

V. Navda et al [5] investigated the possibility of implementing channel hopping inside 802.11 to secure a legitimate to goodness communication from jamming endeavors. They started by assessing the best channel examining and jamming technique that a jammer can use to decrease the throughput of a legitimate communication that uses channel hopping to oppose jamming, and afterward investigated how to best tune the channel hopping method to oppose such a brilliant jammer.

C. Popper et al [6] concentrated on a related however distinctive issue for broadcast communication: How to empower robust against jamming broadcast without shared secret keys? As an answer for the portrayed issue, they propose a plan called Uncoordinated DSSS (UDSSS) that empowers authentic spread-spectrum against jamming broadcast without the prerequisite of shared secrets. UDSSS keeps unscrupulous collectors from meddling with the communication (to different recipients) while it empowers them to get the data themselves. After a certain time, each beneficiary will succeed in distinguishing the right spreading code and its synchronization, along these lines dispreading the sign.

In [7], A. L. Toledo and X. Wang presenting a mechanism for non parametric detection method for MAC layer DOS attacks which does not required any modification of the existing system. The method is based on the M truncated sequential kolmogorov Smirnov statistics, observe the successful transmission and the collisions of the terminal in the network, and determines how explainable the collisions are given This method has a very short detection latency and high detection accuracy.

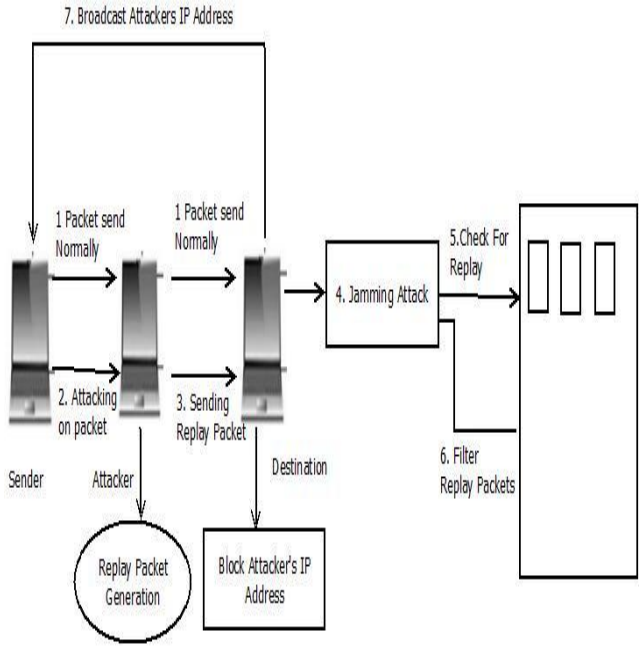
In [8], A. Hamieh and J. Ben-Othman consider one of DOS attacks term as Jamming. Interfacing with legitimate wireless communication is one of the main objectives of the jammer. A jammer can achieve the goal by either prevent a real traffic source from sending out a packet or by prevent the reception of legitimate packets. Author proposed a novel method for detecting such type of attacks by measuring of error distribution.

In [9], proposed and experiment with the plan of configurable link layer security framework of wireless sensor network. The author also evaluated numerous aspects related to the configurable block cipher modes of operations, configurable MAC sizes and configurable replay protection. W. Xu et al [10] studied different types of jamming attacks and measures the effectiveness of jammer using packet sent ratio and packet delivery ratio but only measurement is not enough to classify the presence of a jamming attack. They have proposed the enhanced detection techniques signal strength consistency check and location consistency check.

3. Implementation Details

In this paper, we provided an in-depth study on the impact of jamming and replay packet attacks on the wireless sensor applications. We design the system to achieve efficient and robust jamming and replay packet attack detection. We design algorithm for detection of jamming attack also block actual attacker.

3.1 System Architecture



1: System Architecture

The mutual nature of wireless channels is susceptible to jamming attacks, which broadcast radio interference to affect the network availability of electronic equipments. It is very easy to launch jamming attack but it is hard to detect. A novel method is proposed as a solution to avoid the jamming attack. It also helps in detection and prevention of other attacks like Replay attack and blocking IP address of actual attacker in the network. Prevention is done by filtering the replay packet which is responsible for time critical network Jamming and Delay.

We are presenting a novel technique to preserve the wireless network from not only the Jamming attacks, but also against the Replay attacks. This technique can detect the jamming and Replay attacks, and also provides the means to reduce them.

The methodology is divided into five different modules. They are sender, attacker, Jamming detection, Replay detection, and receiver module. The sender module chose the file to be sent, then divide it into packets, and send these packets over the network. The attacker module introduces the jamming attack in the network, and duplicates the sent packets and sends copies of it in the

Licensed Under Creative Commons Attribution CC BY

network. The Jamming and Replay detection modules detect the two attacks in the network, and takes needful actions to recover the system. Finally, the Receiver module receives the packets from the network. Later, deletes the duplicate packets and retrieves the original packets.

3.2 Algorithm

For Jamming attack

1: At Sender:
2: For each packet
3: {
4: T1 = Calculate current time stamp for packet send;
5:P1= Processing time
6: Send (Packet +T);
7: Send (Packet +T1, P1, H(T1), H(P1));
8 :}
9: At Receiver:
10: {
11: T2 = calculate time stamp when packet received.
12: Calculate Tdiff = T2-T1;
13: Calculate Pdiff=P1-P2;
14: Threshold Thr = previously measured;
15: if (Tdiff <Thr)
16: {
17: Packet received normally.
18 :}
19: else if(Pdiff >KDC(Thr))
20:{
21: Network is Jammed.
22:}
23 :}

3.3 Mathematical Model

1) At Sender Timestamp (Ts) is calculated for each sending packet

$T_s = \sum_{i=1}^{N} (Pi)$
Where Pi are sending packet and
Timestamp (T_s) - Time at which packet send.

2) Calculate Time stamp (Td) for each receiving packet

$T_d = \sum_{i=1}^{N} (Ri)$
Where Ri are Receiving packet and
Timestamp (T_d) - Time at which packets are received.

3) R is the set of receiving packets.

R = (R1, R2, R3... Rn).
Timestamp (Tr) - Time at which packets are received.
Threshold is calculated for Jamming detection.
4) Calculate Threshold T_{sd} :

$T_{sd} = \sum_{i=i}^{N} T_d - \sum_{i=i}^{N} T_s$

Where, Td and Ts are the time stamps for all packets at receiver and sender respectively. For each communication the Time for the entire packet sending is calculated and this time is compared with the generated threshold Tsd.

5) Calculate Processing Time P_t:

$$P_t = \sum_{i=1}^{N} (Pti)$$

Where Pti are processing time of sender, attackers and receiver.

6) The End to End Delay can be calculated as follows

$D = \sum_{i=0}^{N} (di)$
N is the number of transmissions.
di is the delay for i-th transmission.

4. Result and Discussion

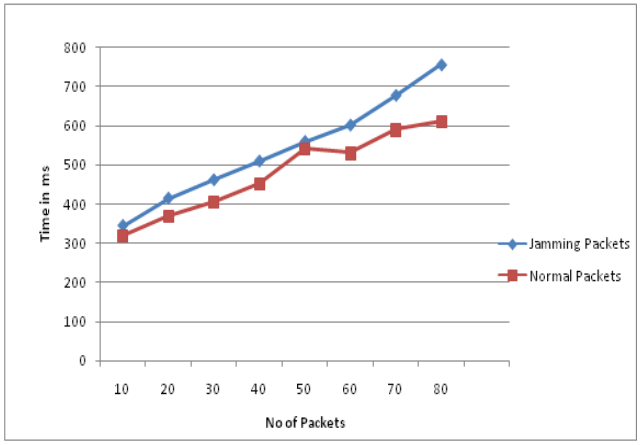


Figure 2: Number of packets Vs time

The figure 2 shows number of packets vs time graph in which the time required for the transmission of no of packet for normal transmission and with jamming transmission of packets. With jamming attack transmission packet requires more time for the transmission as the attacker may hold the packets during packet forwarding through intermediate node.

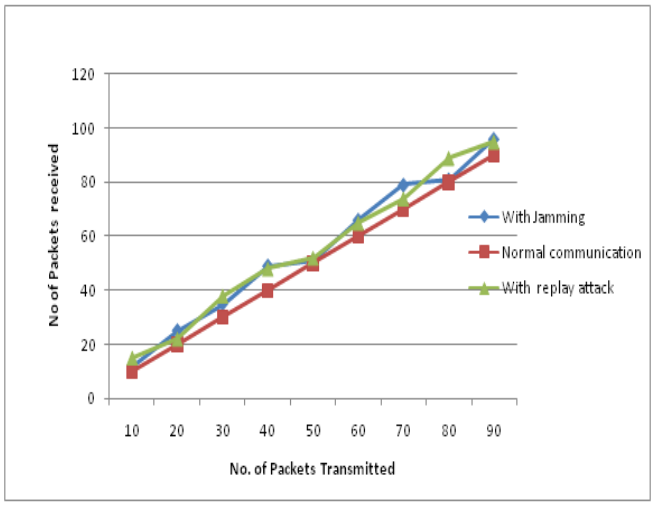


Figure 3: Number of packet received and forwarded

Licensed Under Creative Commons Attribution CC BY

The figure 3 shows the packet forwarded from sender vs the packet received at receiver for all the three types of communication with Jamming attack, replay attack and with normal communication. As the jamming attack only holds the packet and replay attack holds the data and makes duplicate copy of packets and forwarded to the receiver. And hence for the replay attack no of packets received at receiver is more.

5. Conclusion

Detecting Jamming is the first step in defeating it. Here we are discussed about our proposed method for the attack detection. We propose algorithm which are jamming attack detection algorithm. In the proposed algorithm we also try to detect the attacker node, block the attacker node and broadcast the ID of the attacker node through the network to prevent the attack.

Reference

[1] Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless applications Zhuo Lu, Student Member, IEEE, Wenye Wang, Senior Member, IEEE, and Cliff Wang, Senior Member, IEEE, August 2014.
[2] S. Malladi, J. Alves-Foss, R. B. Heckendorn, "On Preventing Replay Attacks on Security Protocols", In Proc. International Conference on Security and Management, 2002.
[3] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks, " in Proc. IEEE INFOCOM, May 2007, pp. 1307-1315.
[4] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming resistant key establishment using uncoordinated frequency hopping, " in Proc. IEEE Symp. Security and Privacy, Washington, DC, USA, May 2008, pp. 64-78.
[5] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks, " in Proc. IEEE INFOCOM, May 2007, pp. 2526-2530.
[6] C. Popper, M. Strasser, and S. Capkun, "Jamming resistant broadcast communication without shared keys, " in Proc. USENIX Security, Berkeley, CA, USA, Aug. 2009.
[7] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks, " IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 347-358, Sep. 2008.
[8] A. Hamieh and J. Ben-Othman, Detection of jamming attacks in wireless ad hoc networks using error distribution, in Proc. IEEE ICC, Dresden, Germany, Jun. 2009.
[9] D. Jinwala, D. Patel, and K. Dasgupta, "FlexiSec: A Configurable Link Layer Security Architecture for Wireless Sensor Networks", presented at CoRR, 2012.
[10] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", in Proc. ACM MobiHoc, Urbana Champaign, IL, USA, 2005, pp. 46-57

Licensed Under Creative Commons Attribution CC BY