International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Jamming and Replay Packet Attack Detection in Time Critical Wireless Application

Pratibha S. Gaikwad[1], S. P. Pingat[2]

[1]PG Student, Pune University, STES's, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

[2]Professor, Pune University, STES's, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: ***In recent few years, the development of digital physical frameworks has grown enormously; because of the fact that, the wireless networking applications has been drawing expansive interest of studies, specifically in the field of Smart Grid. The Digital Physical Frameworks are mainly suitable for the time-critical message transmission in wireless networks. This paper is attributed to the various attacks that are found in the wireless networks, and how these attacks can be detected and prevented in wireless applications. The attacks that we are concentrating are Jamming attack and the Replay attack. The shared and open nature of wireless networks invites the Jamming attacks, which shows the radio obstruction in influencing the system ability. The previous methods that have been proposed till now, are partially successful in detection of these attacks. But the prevention and securing the actual transmitted messages has been the real problem. Thus, we provide a novel method to detect the jamming attacks by use of message invalidation ratios.***

Keywords: Jamming attack detection, wireless network, smart grid applications, time-critical messaging, replay packet attack detection.

1. Introduction

a. Wireless Networks

Wireless communications give both adaptability and expense savings in deployment and maintenance contrasted with wire lined deployments. Wireless can be sent anyplace and whenever. A sensor that has wireless capacities can be effectively migrated and when needed, extra supplementary sensors can be conveyed in many cases within a couple of hours.

As these networks gain fame, providing security and trustworthiness will turn into an issue of basic criticalness. Regular difficulties connected with wireless communications are probabilistic channel behavior, inadvertent and controlled interference or jamming, and eavesdropping or unauthorized modification of the communications if not secured by authentication and encryption. A wireless correspondence system without fitting security protocols can be abused with a man-in-the-middle attack. The result could be both loss of administration and loss of privacy [2].

b. Smart Grid

The National Institute for Standards and Technology (NIST) [7] distributed the smart grid interoperability framework in September 2009. The elements that structure the smart grid are shown by the NIST Framework. Observing information begins in the home, the transmission and distribution networks, and the mass era offices. This information is then supplied into the operations and business applications. Command and control traffic begins in the operations applications and courses through the communication system to the transmission, distribution, and private offices.

In the electric power system, the amount of observing information will regularly surpass the measure of command and control information by a huge variable, on the grounds that there are numerous gadgets being checked. This implies that the volume of communication traffic will be commanded by the information securing needs. Then again, the prerequisite for dependable and quick communications is prone to be commanded by the information outbound from the operations focus, despite the fact that there is less traffic.

c. Jamming Attacks

Albeit a few studies have focused on jamming-style attacks, the meaning of this sort 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 deliberately attempting to interfere with the physical transmission and gathering of wireless communications.

The destination of a jammer is to interfere with true blue wireless communications. A jammer can accomplish this objective by either keeping a genuine traffic source from conveying a bundle, or by keeping the gathering of honest to goodness packets [11].

d. Replay Attacks

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 [9].

In this paper, 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 remaining paper is organized as: Section II gives the brief study about the techniques that have been previously developed in the same field. The Section III gives the detailed contribution of the system that we are proposing. Finally, Section IV concludes the paper.

2. Literature Survey

In this section we survey on different papers related to the wireless application, attacks. In [5], Li et al 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 [6] address and depict the opposition to jamming/key establishment circular dependency issue: 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.

Navada et al [10] contemplated to use channel hopping to make 802.11 networks strong to jamming attacks. The objective is to perceive how significantly all the more versatility 802.11 protocols can be accustomed to jamming attacks. Clearly, imperviousness to a jammer is not generally conceivable subsequent to, in the wireless domain; a jammer with boundless resources can simply effectively jam any wireless transmission by flooding the whole spectrum that could be utilized by the client. The jammer knows all the non-randomized points of interest of the honest to goodness correspondence's versatility procedures, and can plan its jamming convention considering that learning. The target of this framework is then to outline the channel hopping convention that amplifies the true blue correspondence's throughput in the vicinity of this learned jammer.

There are different impedances or issues on immediate sequence spread spectrum communication channel particularly jamming issues, so as to concentrate on this issue an immediate sequence spread spectrum (DSSS) communication framework utilizing Gold code was utilized as point -to-point with completely synchronized in the middle of transmitter and collector under the impact of Additive White Gaussian Noise (AWGN) channel and single tone jamming (STJ) and multi tone jamming (MTJ) [8]. C. Popper et al [2] 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, we 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

3. Proposed Work

The mutual nature of wireless channels is susceptible to jamming attacks, which broadcast radio interference to affect the network availability of electronic equipments. 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.

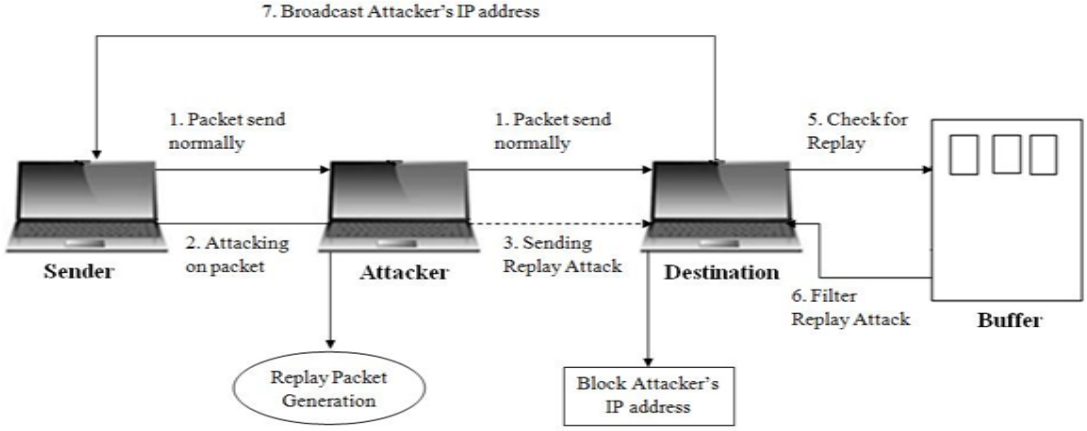

Figure 1: Proposed System Architecture

Table1: Comparison between various attacks

Paper Name	*Analysis*	*Advantages*	*Disadvantages*
Communication Networks and Systems in substations [3].	A large amount of communication traffic is time critical messages in power substations have latency constraints ranging from 3 ms to 500 ms	Addresses most of the issues that migration to the digital world entails.	SAS design engineering is required which can address the challenges for practical implementation.
On network performance evaluation toward the smart grid: A case study of DNP3 over TCP/IP [12].	No guarantee of network availability.	Cost-efficient and backward-compatible communication protocol for the smart grid.	A fine-grained and lightweight network protocol for the smart grid can be implemented.
The feasibility of launching and detecting jamming attacks in wireless networks [11].	No guarantee of on time message delivery.	Focused on both sides of the issue by presenting four different jammer attack model.	PDR presented in this paper cannot differentiate the jamming attack from other network disruptions.
FlexiSec:A Configurable Link Layer Security Architecture for Wireless Sensor Networks [4].	They believe that there is a need for investigating the feasibility of configurable software based link layer security architecture.	FlexiSec is useful in attaining the optimum performance in a deployed application.	Some modes of FlexiSec only support low data rate applications.
Jamming resistant key establishment using uncoordinated frequency hopping [6].	Reactive jammers disrupt legitimate transmissions in a more active and versatile manner than non-reactive jammers.	Solution for cyclic dependency between anti-jamming spread-spectrum communication and key establishment.	Less efficient and less reliable.

4. Conclusion

Security and the efficient message delivery are the important aspects of the wireless network communications. The jamming and replay attacks have been the vital aspect in attacking the wireless networks. There have been many attempts in preserving the network from such attacks, but most of them failed in providing the sufficiency. Thus, we have proposed a novel technique for securing the wireless networks from the jamming and the replay attacks.

Though, we are not claiming to have proposed a complete solution against such attacks, as the new attacking techniques are bound to be developed. Hence, the future studies in this field are inevitable.

References

[1] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, “A survey of wireless communications for the electric power system”, Pacific Northwest National Lab., Richland, WA, USA, Tech. Rep. PNNL-19084, Jan. 2010.
[2] C. Popper, M. Strasser, and S. Capkun, “Jamming resistant broadcast communication without shared keys,” in Proc. USENIX Security, Berkeley, CA, USA, Aug. 2009.
[3] Communication Networks and Systems in Substations, IEC Standard 61850, 2003.
[4] D. Jinwala, D. Patel, and K. Dasgupta, "FlexiSec: A Configurable Link Layer Security Architecture for Wireless Sensor Networks”, presented at CoRR, 2012.
[5] 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.
[6] 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.
[7] Office of the National Coordinator for Smart Grid Interoperability, “NIST framework and roadmap for smart grid interoperability standards, release 1.0”, NIST Special Publication 1108, pp. 1–145, 2009.
[8] S. K. Gharkan, A. A.-E. Noori, S. L. Mohammed, “Performance of Direct Sequence Spread Spectrum System (DSSSS) in Presence of Single and Multi Tone Jamming”, Eng. & Tech. Journal, Vol.31, No.4, 2013.
[9] S. Malladi, J. Alves-Foss, R. B. Heckendorn, “On Preventing Replay Attacks on Security Protocols”, In Proc. International Conference on Security and Management, 2002.
[10] 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.
[11] 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.
[12] X. Lu, Z. Lu, W. Wang, and J. Ma, “On network performance evaluation toward the smart grid: A case study of DNP3 over TCP/IP,” in Proc. IEEE GLOBECOM, Houston, TX, USA, Dec. 2011.