International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

A Review on CSI Based Security Awareness in Wireless Networks

Ayush Nagar[1], Prof. Pankaj Raghuwanshi[2]

ABSTRACT: Conventional computer networks are undergoing a paradigm shift with evolving devices capable of performing computational tasks and storing data. The internet of things can be seen as a broader term encompassing conventional networks, with the connection of multiple smart devices connected over internet. Most of the conventional security mechanisms are reactive in nature whereas for large scale networks, a proactive approach is needed to ensure security. Application layer security alone is NOT reliable and enhanced security measures at the network layer and physical layer need to be augmented, which has seen lesser impetus in existing work. Proactive approaches to detect possible attacks use the channel state information (CSI) of the network. However, limited work has been done in estimating the time varying CSI statistics. Outdated CSI can lead to false alarms regarding attacks. Additionally, crest factor reduction of the data stream can make it imperceptible to potential attackers to pick up data transmissions. This would lead to a much more proactive approach for securing new age IoT networks. This paper presents a review on the various proactive approaches for security aware channel assignment for IoT Networks.

Keywords: Internet of Things (IoT), Intrusion Detection, Proactive Approach, Security Aware Channel Assignment, Throughput.

I. INTRODUCTION

Nowadays, smart devices connected over the internet or a local network can be termed as a network contrary to the conventional networks which comprised of only conventional computers connected together. Moreover, there has been a deliberate migration of networks from wired to the wireless domain due to the following reasons [1]:

- Enhanced Mobility.
- Ease of Maintenance.
- Ease of scaling (up-scaling or down-scaling)

However, these benefits have their associated challenges as the absence of a dedicated guided medium (channel) allows attackers or intruders to penetrate the network more easily.

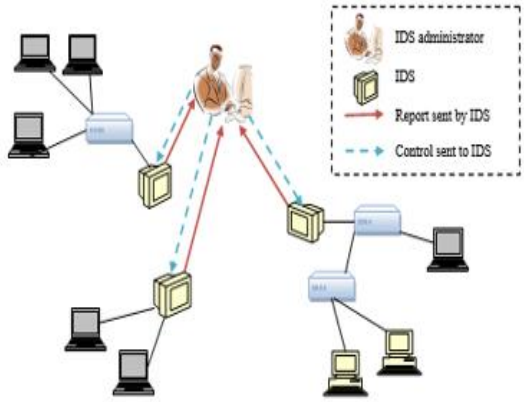


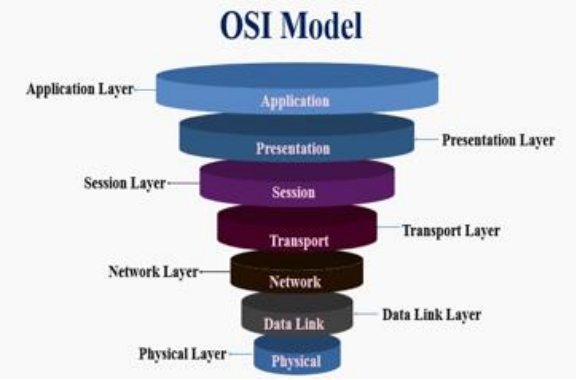
Fig.1 Conventional Intrusion Detection System

Protecting IoT objects necessitates a general security framework - which is a challenging task indeed - covering all IoT assets and their corresponding possible attacks in more details. Therefore, it is absolutely essential to identify all attacks against security or privacy of IoT assets, which is the first step towards developing such framework. Having said that, IoT ecosystem, without doubt, is very complex and confusing, especially when it comes to precisely defining its main assets. Referring to conventional techniques has shown several IoT threat models based on IoT assets, none of which has introduced a comprehensive IoT attack model along with compromised security goals for such a highly intricate system. Network intrusion detection systems (in short NIDS) are systems designed to gauge and analyze the intrusions targeted towards networks. These systems are placed at specific places within the network to monitor every type of traffic that passes through the network. All kinds of traffic that comes to and goes from the network is sensed for any sort of malicious activity or intrusion.
There are 3 primary security paradigms in IoT networks:

1) Application Layer Security
2) Network Layer Security
3) Physical Later Security

Application level security corresponds to securing the system against attacks over malicious applications. This level of security can be bypassed in case the intruder attacks the

lower levels of the OSI Layer.



.

Fig.2 The OSI Model

2. Reactive versus Proactive Approaches

The conventional intrusion detection systems aims at detecting malicious activity in networks and conducts forensic analysis once attack is over. It monitors network resources to detect intrusions and attacks that were not stopped by preventative techniques. An intrusion is an attempt to compromise the confidentiality, integrity or availability of a system. Intrusion detection systems can be considered to be a crude analogy to burglar alarms in real life. Misuse- based IDSs are designed to detect violations to predefined security policies. However, the matter gets complicated with the introduction of possible malicious behaviors which cannot be specified precisely ahead of time. Statistical anomaly detection was introduced for this particular reason where a profile of a user or a system is created and any deviations from the profile are reported. However, for large scale IoT networks, the computational complexity at the network gateway becomes so large, that securing all possible nodes of the network is infeasible ahead of time. Hence a proactive approach is needed, and conventional intrusion detection systems (IDS) do not suffice. The next section presents the relevant literature review in the domain. The challenging issues pertaining to design of any intrusion detection system are [2]:

- Limited Efficiency: To evaluate the activities in real time IDSs (proactive) are needed. It is very hard need to meet the requirements when

faced with a very large number of events of large data transfers, as is typical in today's IoT networks. Hence conventional IDSs usually slow down a system where as NIDSs drop network packets for those there is no sufficient time to process.

- High Number of False Positives: Most IDSs detect attacks throughout an enterprise by analyzing information from a single host, a single application, or a single network interface, at many locations throughout the network. False alarms are high and attack recognition is not perfect. Lowering thresholds to reduce false alarms raises the number of attacks that get through undetected as false negatives. Improving the ability of an ID to detect attacks accurately is the primary problem facing IDS manufactures today.
- Burdensome Maintenance: There are some requirements specific knowledge as well as substantial efforts to configure and maintain the IDSs usually. Here some examples like, misuse detection where usually for their implementation expert system shells that encode and match signatures using rule sets are used. Upgrading these rule sets involves details peculiar to the expert system and its language for expressing rules sets, and it may only permit an indirect specification of the sequential interrelationships between events. These considerations are also applied to the addition of a statistical metric, typically used to find unusual deviations in nature.
- Limited Flexibility: If an Intrusion detection system has been developed for a typically specific environment then it may hard to use in other environments whether it consists of same kind of concern as well as policies. The mechanism used for detection may also face hardships to adapt to different patterns of usage. The tailoring detection method specifically to the system with some if and buts replacing those over time with improved detection techniques are also problematic with many IDS implementations. Often the IDS needs to be completely restarted in order to make changes and additions take effect.
- End-to-end Encryption: By improving security concerns in protocols used for communications in end to end mode encrypted traffic availability gets risen. Besides

opposing a secret listening, encrypted content keeps network-based IDS from viewing into packets and analyzing their contents for intrusions.

- High Data Rate Requirements: By increasing communication traffic rate the processing speed also changes because communication traffic rate is directly proportional to processing speed. So, it is needed to analyze the contents of communication packets. Here potentially packet loss occurs. In NIDS to observe various communication streams simultaneously increases the difficulty when switched communication i.e. a conventional communication is used in place of broadcast communication.
- Breadth of Attacks: By conceiving newer attacks, IDS needs to be updated for finding them. Until frequently newer attacks appended and older one dropped. Hence, there

is a need of a detection algorithm for huge attack coverage large span of processing time.

- Insufficiency of Conventional Methods: Common security mechanisms employing application level / bit level encryption algorithms are becoming less secure due to the increasing computational capability of machines based on AI and Quantum Computing, Encryption thus alone CAN NOT prove to be secure.

Additional resource based challenges include [3]:

- Heterogeneous network configurations making enumerating system-specific detection parameters for each system extremely time consuming.
- Increased number of critical nodes in the network increasing the performance overhead.
- Large system overheads due to additional activities for security such as logging or extraction CSI.
- Difficulty in recognizing network-wide attacks for hosts with insufficient computational capability to deploy complete host-based IDS.

The major challenge of securing any network arises due to the following fundamental reasons:

1) Conventional security in terms of cryptographic algorithms are NOT completely secure.
2) Cryptography relies on the infeasibility of computers to perform a computational operation within a specific time due to its computational complexity. However, with the emergence of Quantum Computing, the future scenario can completely change with the "Hack now, decode later approach"- (Source: MIT Tech Review).

3) It is infeasible to search for any intrusion detection system to find all possible loopholes while traversing the entire periphery of the network.
4) Moreover, in case of IoT, there is a large diversity of devices with varying levels of memory and computational power, making complex cryptographic algorithms infeasible to be implemented on them (although the advanced cryptographic algorithms are NOT completely secure too.)
5) There always remains a tradeoff among the level of security and computational power needed thereby constraining system performance.

To sense the channel and obtain the channel state information (CSI) of the system, the periodic sensing of the channel needs to be done based on the transmission of data packets. Let the data packet before transmission be designated by y and the one at the receiving end be designated by y' [4]:

The comparison between y *and* y' is done based on the auto-correlation function C_{auto} given by:

$$\boldsymbol{C_{auto} = \frac{1}{t1 - t2}\int_{t1}^{t2} y(t).y'(t)dt}$$

Three basic outcomes are possible as a result of the evaluation of the auto-correlation function which are:

Low Jamming Attacks: $\boldsymbol{\tilde{E}\{C_{auto}\ is\ high: \tilde{E}\{y'(t)\} \leq 1.5\ \tilde{E}\{y(t)\}}$

Moderate Jamming Attacks:
$\boldsymbol{\tilde{E}\{C_{auto}\ is\ moderate: \tilde{E}\{1.5y(t)\} \leq E\{y'(t)\} \leq 2\ \tilde{E}\{y(t)\}}$

High Jamming Attacks: $\boldsymbol{\tilde{E}\{C_{auto}\ is\ low: \tilde{E}\{y'(t)\} \geq 2\ \tilde{E}\{y(t)\}}$

Here $\tilde{E}$ denotes the energy function
However, intelligent attackers change the bandwidth of attack and hence it is necessary to repeat the CSMA-CD protocol periodically over time.

3. Literature Review

This section highlights the recent advances in the field of IoT intrusion detection at the network layer and mitigation mechanisms:

Germain et al. [5] proposed that channel state information offers a unique characteristic that can be used for authenticating devices at the physical layer. The quickly changing response of the mobile channel presents a challenge for identifying trusted transmitters. Authors propose the use of recurrent neural networks to predict these changes in order to make an authentication decision. Using previous channel response measurements, the approach can condition the output of the network and estimate future channel responses. This work presents a novel method for physical layer authentication using two variations of a conditional generative adversarial network (CGAN) and evaluates the CGAN accuracy against networks using long short-term memory (LSTM) and gated recurrent unit (GRU) cells.

Salameh et al. [6] showed that Cognitive radio networks (CRNs) have a great potential in supporting time-critical data delivery among the Internet of Things (IoT) devices and for emerging applications such as smart cities. However, the unique characteristics of different technologies and shared

radio operating environment can significantly impact network availability. Hence, in this paper, we study the channel assignment problem in time-critical IoT-based CRNs under proactive jamming attacks. Specifically, we propose a probabilistic spectrum assignment algorithm that aims at minimizing the packet invalidity ratio of each cognitive radio (CR) transmission subject to delay constrains. We exploit the statistical information of licensed users' activities, fading conditions, and jamming attacks over idle channels. Simulation results indicate that network performance can be significantly improved by using a security- availability- and quality-aware channel assignment that provides communicating CR pair with the most secured channel of the lowest invalidity ratio.

Chen et al. [7] proposed investigate physical layer security (PLS) in non-orthogonal multiple access-enabled (NOMA-enabled) underlay cognitive radio networks (CRNs) with outdated channel state information (CSI). Considering the influence of outdated CSI on the interference of secondary transmitter (Alice) to primary user (PU), the constraint for the power is adopted to guarantee the quality-of-service (QoS) of PU over Nakagami-m channels. To further analyze the NOMA-enabled underlay CRNs with outdated CSI in PLS perspective, the secrecy performance is evaluated by the closed-form expressions for connection outage probability (COP), the intercept probability (IP) and effective secrecy throughput (EST). In addition, Monte Carlo simulations are provided to verify the derived analytical results.

Shen et al. [8] proposed chaotic mapping uses a modified three-dimensional Lorenz mapping, adding feedback factors to the common Lorenz mapping, which generates 3 masking factors, and uniformly encrypts the three dimensions (3D) of the constellation diagram, subcarrier frequency, and symbols, which effectively improves the security of the system. Owing to the linearity of the (inverse) fast Fourier transform (FFT/IFFT) operation in the OFDM system and the mismatch between the number of subcarriers and the number of Fourier points, the use of idle subcarriers in the FFT/IFFT operation can reduce peak-to-average power ratio (PAPR). The proposed high-security OFDM-PON is experimentally verified based on the PAPR values.

Ahmed et al. [9] presented a systematic and comprehensive review on security and authentication in the internet of things (IoT) framework addressing current challenges and future directions of research. The authors showed that existing authorization and authentication schemes are not sufficient for handling security, due to the scale of the IoT networks and the resource- constrained nature of devices. In order to overcome challenges due to various constraints of IoT networks, there is a significant interest in using machine learning techniques to assist in the authentication and authorization process for IoT. In this paper, recent advances in authentication and authorization techniques for IoT networks are reviewed. Based on the review, we present a taxonomy of authentication and authorization schemes in IoT focusing on machine learning-based schemes. Using the presented taxonomy, a thorough analysis is provided of the authentication and authorization (AA) security threats and challenges for IoT. Furthermore, various criteria to achieve a high degree of AA resiliency in IoT implementations to enhance IoT security are evaluated. Lastly, a detailed discussion on open issues, challenges, and future research directions is presented for enabling secure communication among IoT nodes.

Sadique et al. [10] proposed an intertwining logistic map (ILM)-cosine transform aided encryption algorithm combined with artificial noise enhancing physical layer security (PLS) is introduced. Also walsh-hadamard transform technique integrated with QR-decomposition based zero forcing (ZF) block diagonalization (QR-ZF-BD) precoding for multi-user interference reduction and non-iterative clipping and filtering technique for peak to average power ratio (PAPR) reduction are utilized. In addition, Low density parity check (LDPC) and repeat and accumulate (RA) channel coding with cholesky decomposition based ZF and minimum mean square error signal detection schemes for improved bit error rate (BER) are also introduced.

Zhao et al. [11] proposed security of an orthogonal frequency division multiplexed passive optical network (OFDM-PON) based on four dimensional (4D) encryption, including constellation, subcarrier, symbol and time, which is proposed for the first time in this paper. 4D-hyperchaotic mapping is used to generate four masking factors to achieve ultra-high security encryption in four different dimensions. During the encryption, dimension coordination optimization is adopted, which effectively reduces the time cost of the system and improves the encryption efficiency by 3 times. At the same time, probabilistic shaping (PS) technology is used to further optimize the system that has effectively improved the bit error performance by about 1 dB. The proposed encryption technique for OFDM-PON has been demonstrated successfully with the help of experiments.

Ferdowai et al. [12] proposed a statistical feature based watermarking algorithm is proposed for dynamic authentication of IoT signals to detect cyber-attacks. The proposed watermarking algorithm, based on a deep learning long short-term memory structure, enables the IoT devices (IoTDs) to extract a set of stochastic features from their generated signal and dynamically watermark these features into the signal. This method enables the IoT gateway, which collects signals from the IoTDs, to effectively authenticate

the reliability of the signals. Moreover, in massive IoT scenarios, since the gateway cannot authenticate all of the IoTDs simultaneously due to computational limitations, a game-theoretic framework is proposed to improve the gateway's decision making process by predicting vulnerable IoTDs. The mixed-strategy Nash equilibrium (MSNE) for this game is derived, and the uniqueness of the expected utility at the equilibrium is proven. In the massive IoT system, due to the large set of available actions for the gateway, the MSNE is shown to be analytically challenging to derive, and thus, a learning algorithm that converges to the MSNE is proposed.

Burton et al. [13] proposed a data exfiltration method using Channel State Information (CSI) from ambient WiFi data. Modulation is performed by modifying the environment by moving a physically actuated machine resulting in a change to the channel response that is measurable by a distant receiver capable of collecting CSI samples. An attacker can use this to exfiltrate data when transmission using conventional methods is impossible, yet the attacker controls a moving mechanism. Authors discuss the design of the covert channel in detail and produce a proof of concept implementation to evaluate the performance in terms of communication quality. The results suggest that even a simple implementation provides robust network environments.

Li et al. [14] proposed an IoT feature extraction and intrusion detection algorithm for intelligent city based on deep migration learning model, which combines deep learning model with intrusion detection technology. According to the existing literature and algorithms, this paper introduces the modeling scheme of migration learning model and data feature extraction. In the experimental part, KDD CUP 99 was selected as the experimental data set, and 10% of the data was used as training data. At the same time, the proposed algorithm is compared with the existing algorithms. The experimental results show that the proposed algorithm has shorter detection time and higher detection efficiency.

Conclusion

It can be concluded from the previous discussions that Internet of Things (IoT) networks are wide area networks typically connecting multiple type of devices. IoT networks share common resources such as bandwidth or spectrum among several users or stations. Due to continued sharing of resources, IoT networks often come under security attacks, most common of which are jamming attacks. In the case of jamming attacks, deliberately designed random jamming signals are added to the channel. These jamming signals along with noise result in packet losses and low throughput, degrading the overall performance of the IoT. This paper presents a review of the proactive approaches for security aware channel assignment in IoT networks.

References:

1. Pecorella, L Brilli, L Mucchi, “The role of physical layer security in IoT: A novel perspective”, Journal of Inforamtion, MDPI 2016, vol. 7, no. 3, pp.1-17
2. K. Kalkan and S. Zeadally, "Securing Internet of Things with Software Defined Networking," in IEEE Communications Magazine, vol. 56, no. 9, pp. 186-192, Sept. 2018.
3. M. Sarrab and S. M. Alnaeli, "Critical Aspects Pertaining Security of IoT Application Level Software Systems," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 960-964.
4. H. -M. Wang, J. Bai and L. Dong, "Intelligent Reflecting Surfaces Assisted Secure Transmission Without Eavesdropper's CSI," in IEEE Signal Processing Letters, vol. 27, pp. 1300-1304, 2020.
5. K. S. Germain and F. Kragh, "Mobile Physical-Layer Authentication Using Channel State Information and Conditional Recurrent Neural Networks," 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), 2021, pp. 1-6.
6. H. B. Salameh, S. Almajali, M. Ayyash and H. Elgala, "Security-aware channel assignment in IoT-based cognitive radio networks for time-critical applications, IEEE Access 2021, pp.43-47.
7. Y. Chen, T. Zhang, Y. Liu and X. Qiao, "Physical Layer Security in NOMA-Enabled Cognitive Radio Networks With Outdated Channel State Information," in IEEE Access, vol. 8, pp. 159480-159492, 2020.
8. J. Shen Bo Liu; Yaya Mao; Rahat Ullah; Jianxin Ren; Jianye Zhao; Shuaidong Chen., "Enhancing the Reliability and Security of OFDM-PON Using Modified Lorenz Chaos

Based on the Linear Properties of FFT," in Journal of Lightwave Technology, vol. 39, no. 13, pp. 4294-4299, July1, 2021.

9. Kazi Istiaque Ahmed, Mohammad Tahir, Mohamed Hadi Habaebi, Sian Lun Lau, Abdul Ahad "Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction", MDPI 2021, vol.21, issue.5122, pp. 1-34.
10. J. J. Sadique, S. E. Ullah, M. R. Islam, R. Raad, A. Z. Kouzani and M. A. P. Mahmud, "Transceiver Design for Full-Duplex UAV Based Zero-Padded OFDM System With Physical Layer Security," in IEEE Access, vol. 9, pp. 59432-59445, 2021
11. J Zhao, B Liu, Y Mao, R Ullah, J Ren, S Chen, High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization", OSA publications, vol.28, issue.14, pp.21236-21246.
12. A. Ferdowsi and W. Saad, "Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems," in IEEE Transactions on Communications, vol. 67, no. 2, pp. 1371-1387, Feb. 2019.
13. T Burton, K Rasmussen, "Private Data Exfiltration from Cyber-Physical Systems Using Channel State Information", in Proceedings of Private Data Exfiltration from Cyber- Physical Systems Using Channel State Information, ACM 2021, pp.223-235.
14. D Li, L Deng, M Lee, H Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning", International Journal of Information Management, Elsevier 2019, vol.49, pp. 533-545.