A Survey on Problems Faced in Identification of Malicious Data Insertion in Wireless Sensor Networks and Rectification of It

Rohini Divase[1], S. N. Kini[2]

[1]ME Computer (Engineering), Jayawantrao Sawant College of Engineering, Hadapsar Pune-411028, Savitribai Phule Pune University, Pune, India

[2]Professor, Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar Pune 411028, Savitribai Phule Pune University, Pune, India

Abstract: ***The purpose of this survey is to present overview of approaches to detecting malicious data injections in wireless sensor network. It also discusses the advantages and disadvantages of different detection methods and compare different approaches them. Wireless sensor networks (WSNs) are defenseless and can be maliciously traded off, either physically or remotely, with potentially devastating impacts. At the point when sensor systems are utilized to recognize the occurrence of events, for example, fires, intruders, or heart attacks, malicious data can be injected to create fake events, and along these lines trigger an undesired reaction, or to cover the occurrence of actual events. Therefore there is a need to identify malicious data injections and build measurement estimates that are resistant to several compromised sensors even when they collude in the attack either willingly or under duress.***

Keywords: Malicious Data Injection, Detection, Wireless Sensor Network, Mining and statistical methods, security management, ad hoc and sensor networks.

1. Introduction

Wireless Sensor Networks (WSNs) can give effective also, financially viable solutions for a substantial assortment of applications, for example, health monitoring, scientific data gathering, environmental monitoring, and military operations. Then again, sensor nodes in these applications could be effortlessly traded off and can inject self-assertively distorted qualities into the networks.

WSNs are regularly used to detect events occurring in the physical space acrossdiverse applications, for example, military surveillance, wellbeing, and environment (e.g., volcano) monitoring. In spite of the fact that these applications have diverse tasks, they all gather sensor measurements and interpret them to identify events, i.e., specific states of interest followed by a remedial response. Such reaction may have significant outcomes and expense. In this manner, the estimations driving to the event detection turn into a basic asset to secure.

When the estimations are somehow replaced or modified by an attacker, they manage malicious data injections. The attacker maymake utilization of the injected data to evoke an occasion reaction, for example, departure on account of flame, when no occasion has happened, or veil the event of a genuine occasion, for example, the trigger for an intrusion alert. Diverse means for acquiring control over the estimations are conceivable.A large number of the studies in the literature address physical and network layer threats by securing the integrity of the measurements amid their transmission (e.g., with a cryptographic hash function). However attacks may trade off the estimations even some time recently they are transmitted. For instance, an attacker may alter with a sensor in the field and load software that reports false estimations. Another probability is that the attacker controls environment by utilizing for case a lighter to trigger a fire alarm.

2. Literature Survey

D. Zhang and D. Liu [1] present a software confirmation plan for dynamic data integrity based on data boundary integrity. It automatically transforms the source code and embeds data guards to track runtime program information. A data guard is unrecoverable once it is corrupted by an attacker, regardless of the possibility that the attacker fully controls the framework later. The corruption of any data guard at runtime can be remotely identified. A corruption either demonstrates a software attack or a bug in the software that needs immediate attention. The advantages of the proposed confirmation plan are as per the following. In the first place, it doesn't depend on any extra hardware support, making it suitable for low cost sensor nodes. Second, it presents minimal communication cost and has adjustable runtime memory overhead. Third, it works even if sensor nodes use different hardware platforms, as long as they run the same software.

B. Sun, X. Shan, K. Wu, and Y. Xiao [2], they first propose integration of framework monitoring modules and intrusion detection modules in the context of WSNs. They propose an Extended Kalman Filter (EKF) based mechanism to recognize false injected data. In particular, by monitoring behaviors of its neighbors and utilizing EKF to predict their future states (genuine in-network aggregated values), every node goes for setting up a normal range of the neighbors' future transmitted aggregated values. This task is challenging due to conceivably high packet loss rate, harsh environment, sensing uncertainty, and so forth. They outline how to use EKF to address this challenge to make effective local detection mechanisms. Utilizing distinctive aggregation functions (average, sum, max, and min), they display how to get a theoretical threshold. They further apply an algorithm of combining Cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) to increase detection sensitivity.

Y. Liu, P. Ning, and M. K. Reiter [3], they present a new class of attacks, called false data injection attacks, against state estimation in electric power matrices. They demonstrate that an attacker can misuse the configuration of a power framework to launch such attacks to effectively introduce arbitrary errors into certain state variables while bypassing existing methods for terrible measurement recognition. In addition, they look at two reasonable attack situations, in which the attacker is either compelled to some specific meters (because of the physical security of the meters), on the other hand restricted in the assets required to compromise meters. They demonstrate that the attacker can systematically and proficiently construct attack vectors in both situations, which cannot just change the results of state estimation, additionally modify the outcomes in arbitrary ways. Even though these work carried out in electric power grid they have made a point which is more relevant in the case wireless sensor networks (WSNs) & hence a proper treatment of the same is essential.

F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho [4] propose a highly adaptable cluster-based „hierarchical trust management protocol for wireless sensor networks (WSNs) to adequately manage selfish or malicious nodes. Unlike prior work, they consider multidimensional trust attributes determined from communication and social networks to assess the overall trust of a sensor node. By method for a novel probability model, they describe a heterogeneous WSN containing an extensive number of sensor nodes with immeasurably distinctive social and quality of service (QoS) behaviors with the goal to yield "ground truth" node status. This serves as a premise for accepting their protocol design by comparing at subjective trust created as a result of protocol execution at runtime against objective trust acquired from actual node status.

Y. Zhang *et al*[5]accurate analysis and decision-making relies on the quality of WSN data as well as on the additional information and context. Raw observations collected from sensor nodes, however, may have low data quality and reliability due to limited WSN resources and harsh deployment environments. This article addresses the quality of WSN data focusing on outlier detection. These are defined as observations that do not conform to the expected behavior of the data. The developed methodology is based on time-series analysis and geostatistics.

M. Mathews, M. Song, S. Shetty, and R. McKenzie[6] While wireless sensor networks are proving to be a versatile tool, many of the applications in which they are implemented have sensitive data. In other words, security is crucial in many of these applications. Once a sensor node has been compromised, the security of the network degrades quickly if there are not measures taken to deal with this event. There have been many approaches researched to tackle the issue. In this paper, we look into an anomaly-based intrusion detection system to detect compromised nodes in wireless sensor networks. An algorithm to detect the compromised sensor nodes has been developed.

A. Liu and P. Ning[7] present the design, implementation, and evaluation of Tiny ECC, a configurable library for ECC operations in wireless sensor networks. The primary objective of Tiny ECC is to provide a ready-to-use, publicly available software package for ECC-based PKC operations that can be flexibly configured and integrated into sensor network applications. TinyECC provides a number of optimization switches, which can turn specific optimizations on or off based on developers‟ needs.

O. Salem, Y. Liu, A. Mehaoua, and R. Boutaba[8], we propose a lightweight approach for online detection of faulty measurements by analyzing the data collected from medical wireless body area networks. The proposed framework performs sequential data analysis using a smart phone as a base station, and takes into account the constrained resources of the smart phone, such as processing power and storage capacity. The main objective is to raise alarms only when patients enter in an emergency situation, and to discard false alarms triggered by faulty measurements or ill-behaved sensors. The proposed approach is based on the Haar wavelet decomposition, non-seasonal Holt–Winters forecasting, and the Hampel filter for spatial analysis, and on for temporal analysis. Our objective is to reduce false alarms resulting from unreliable measurements and to reduce unnecessary healthcare intervention.

A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla[9] present SCUBA (Secure Code Update By Attestation),for detecting and recovering compromised nodes in sensor networks. The SCUBA protocol enables the design of a sensor network that can detect compromised nodes without false negatives, and either repair them through code updates, or revoke the compromised nodes. The SCUBA protocol represents a promising approach for designing secure sensor networks by proposing a first approach for automatic recovery of compromised sensor nodes. The SCUBA protocol is based on ICE (Indisputable Code Execution),a primitive we introduce to dynamically establish a trusted code base on a remote, untrusted sensor node.

F. Liu, X. Cheng, and D. Chen [10] though destructive to network functions, insider attackers are not detectable with only the classic cryptography based techniques. Many mission-critic sensor network applications demand an effective, light, flexible algorithm for internal adversary identification with only localized information available. The insider attacker detection scheme proposed in this paper meets all the requirements by exploring the spatial correlation existent among the networking behaviors of sensors in close proximity. Our work is exploratory in that the proposed algorithm considers multiple attributes simultaneously in node behavior evaluation, with no requirement on a prior knowledge about normal/malicious sensor activities. Moreover, it is application friendly, which employs original measurements from sensors and can be employed to monitor many aspects of sensor networking behaviors.

Paper Name	Author	Work	Advantages	Disadvantages
DataGuard: Dynamic data attestation in wirelesssensor networks[1]	D. Zhang and D. Liu,	Proposed dynamic data attestation in wireless sensor networks based on data boundary integrity.	It is feasible and effective.	cannot detect attacks that do notcorrupt data guard values.
Anomaly detection based secure in-network aggregation for wireless sensor networks[2]	B. Sun, X. Shan, K. Wu, and Y. Xiao	Proposed that Intrusion Detection Modules (IDM) and System Monitoring Modules (SMM) should work together in order to provide intrusion detection capabilities for WSNs.	It is suitable to provide intrusion detection capabilities for secure in-network aggregation in wireless sensor networks.	evaluated in a single deployment or application setting, or even on a single simulated dataset
False data injection attacks against state estimation in electric power grids[3]	Y. Liu, P. Ning, and M. K. Reiter	Present a new class of attacks, called false data injection attacks, against state estimation in electric power grids.	Indicate that security protection of the electric power grid mustbe revisited when there are potentially malicious attacks.	Not work on investigate the possibility of adapting network anomaly detection techniques to identify false data injection attacks.
Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[4]	F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho	Proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trustand QoS trust.	trust-based IDS algorithm out performs traditional anomaly-based IDS techniques in the detection probability while maintaining sufficiently low false positives.	Required devising and validating a decentralized trust management scheme for autonomous WSNs without base stations
Statistics-based outlier detection for wireless sensor networks[5]	Y. Zhang *et al.*	Addresses the quality of WSN data focusing on outlier detection.	This provides a usable and important tool in a novel scientific field.	Not focus on accuracy assessment for distinguishing between errors and events.
Insider attacker detection in wireless sensor networks[10]	F. Liu, X. Cheng, and D. Chen	Propose a novel idea of insider attackerdetection in wireless sensor networks.	The algorithm is pure localized, thus scales well to large sensor networks	Detection algorithm can be specialized by exploring the degree of the correlations existent among different aspects of sensor networking behaviors.

3. Conclusion

This paper surveys on different approaches to detecting malicious data injections in wireless sensor network.It also discusses the advantages and disadvantages of some of the previous detection methods and compares them. The focus is on detecting malicious datainjections in event detection WSNs, in particular when collusionbetween compromised sensors occurs either willingly or under duress. We find it essential more so now to have an algorithm that can be customized and be used in different applications, and for different kinds of events. This survey throws light on the necessity to devise and develop a working solution under these circumstances.

References

[1] D. Zhang and D. Liu, "DataGuard: Dynamic data attestation in wirelesssensor networks," in *Proc. IEEE/IFIP Int. Conf. DSN*, 2010,pp. 261–270.

[2] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based securein-network aggregation for wireless sensor networks," *Syst. J.*, vol. 7, no. 1, pp. 13–25, Mar. 2013.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks againststate estimation in electric power grids," *Trans. Inf. Syst. Secur.*, vol. 14,no. 1, pp. 21–32, May 2011.

[4] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust managementfor wireless sensor networks and its applications to trust-basedrouting and intrusion detection," *IEEE Trans. Netw. Service Manage.*,vol. 9, no. 2, pp. 169–183, 2012.

[5] Y. Zhang *et al.*, "Statistics-based outlier detection for wireless sensornetworks," *Int.J. Geogr. Inf. Sci.*, vol. 26, no. 8, pp. 1373-1392, 2012.

[6] M. Mathews, M. Song, S. Shetty, and R. McKenzie, "Detecting compromisednodes in wireless sensor networks," in *Proc. SNPD*, 2007, vol. 1,pp. 273–278.

[7] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curvecryptography in wireless sensor networks," in *Proc. IPSN*, 2008,pp. 245–256.

[8] O. Salem, Y. Liu, A. Mehaoua, and R. Boutaba, "Online anomaly detectionin wireless body area networks for reliable healthcare monitoring,"*J. Biomed. Health Informat.*, vol. 18, no. 5, pp. 1541–1551, Sep. 2014.

[9] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla, "SCUBA: Secure code update by attestation in sensor networks," in *Proc. WorkshopWireless Security*, 2006, pp. 85–94.

[10] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensornetworks," in *Proc. 26th IEEE INFOCOM*, 2007, pp. 1973–1945.

[11] Vittorio P. Illiano and Emil C. Lupu, "Detecting Malicious Data Injections in EventDetection Wireless Sensor Networks", IEEE Transactions OnNetworkAnd Service Management, September 2015.

Author Profile

Ms. Divase Rohini Gopal, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. SavitribaiPhule Pune University, Pune, Maharashtra, India - 411007. She received her B.E (Computer) Degree from Godavari College of engineering, Jalgaon - 425003, India. North Maharashtra University, Pune, Maharashtra, India. Her area of interest is network security,Wireless Sensor Networks.

Prof. Dr. Srinivasa. N. Kini, received his Ph.D. from Cochin University of Science and Technology, Thrikkakara, South Kalamasserry, Cochin. He received his M.E Degree from B.M.S. college of Engineering, Basavanagudi, Bangalore. He received his B.E Degree from K L E Society‟s college of Engineering, Udyambaug Belgaum. He is currently working as Professor at Department of Computer Engineering, JayawantraoSawant College of Engineering, Hadapsar Pune - 411028, India affiliated to SavitribaiPhule Pune University, Pune, Maharashtra, India -411007. His area of interest is Wireless Sensor Networks, Distributed Computing, Network Security and Mobile Computing.