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

Survey on Recent Malicious Data Injection Detection Techniques

Pragati Hadole[1], Vidya Dhamdhere[2]

[1]Computer Engineering, G.H.Raisoni College of Engineering and Management, Pune

[2]Professor, Computer Engineering, G.H.Raisoni College of Engineering and Management, Pune

Abstract: ***Wireless Sensor Networks are used to monitor the environmental parameters, for quick response of event detection. It is used to predict the happening of upcoming events such as, fire alarm system, intrusion detection, heart attack detection systems, military applications etc. But most of the time sensors are compromise by external entities, which arises a serious issue of security in such networks. Such Compromised sensors can report the false readings, which produce the inappropriate and most of the time dangerous responses. So there is a need of system that can appropriately identify the malicious data injected by unauthorized entities at sensor nodes. It is necessary because it is very difficult to detect such malicious data injection attacks on sensor node, if it is occur at multiple sensor nodes simultaneously in network. This paper makes survey of some recent approaches or techniques that are used for malicious data injected nodes in WSN. Also compare these approaches based on various parameters such as technique used, their advantages and limitations. At the end we suggest some research directions which will be used for further study in same field.***

Keywords: Compromised nodes, event detection, wireless sensor network, malicious data injection

1. Introduction

Wireless sensor Networks (WSNs) is a good pretty answer to the problem of grouping information from physical areas, due to their flexibility, low price and simple deployment. Applications of WSNs involve a variety of tasks in each shared and private environments. In shared environments, applications includes infrastructures observations water network, solving road traffic problem, monitoring environmental parameters and surveillance. Personal environments include various applications such as monitoring homes, user activity such as exercise and sleep, and physiological parameters for healthcare.

Event detection is one of the major components in large number of applications in wireless sensor network (WSN). WSNs in military application, there are number of sensor nodes are deployed in particular location to detect the activities of enemy. In health monitoring sensor networks, sensors are deployed to identifypatient's abnormal behavior, in fire detection sensor networks, sensors are used to set up an alarm when any a fire activity starts in that sensor covered area. Even though in specific application, there is need to detect the event before itsactual happening. But like human recognizing events, But just like many other human-recognizable events, the incident offire has no meaning to a sensor node. Therefore, there is a need of suitable technique to pretend the events in such a way that it should be understanding to sensor nodes Therefore the need of exploring such kind of event detection problem in WSN, is arises.

Wireless sensors has a higher risk of being compromised. The sensor nodes deployments are often neglected and they are easy for physically access.Also the use of tamper-resistant hardware in such cases are most of the time too much expensive. Such kind of wireless environment is also very difficult to make secure. There are huge possibility that such sensor nodes get compromised at all layers of the stack protocol. Cryptographic operations and key management requiresvarious computational and power resources. But they cannot work when once a node get compromised. Instead of this, WSNs are stillused in many sectors to monitor various critical infrastructures and human health. In such cases, malicious attacks may lead to significant damage and even loss of life.

In this survey, all approaches assume that the unauthorized outsidermakes undesired effects and injects faulty measurement readings that differ from correct values. This is the assumption which enables the use of data analysis to detect data injections. However, note that the real value that should be reported by compromised sensors is not observable directly. Instead, it can only be characterized from indirect information such as values reported by other sensors, which may or may not be sufficient to detect the compromise. The problem is even more difficult as the indirect information may itself not be correct due to the presence of faults or naturally occurring events.

Faults is any kind of errors, may be transient or not. Such kind of faults are difficult to differfrom a malicious injection faults. Events refer to significant changes in the sensed phenomenon like a fire, earthquake etc. The problem of malicious data injections from events and faults are distinguish from diagnosis and review the state of the art approaches. Another problem of unreliable indirect information is the presence of colluding sensors.In this case,more than one compromised sensor devices producemalicious reading valuesby coordinating with each other. In such situations, the attacker's grasp onthe system is increases, and it will leads to possibilities of the new and more effective kind of attacks. Detection and diagnosis of malicious data injections is a part of anotherproblem of checking the integrity of data sensed by sensors. This data is corruptedby failures or in many other ways. This is studied in this survey, where manytechniques proposed for, faulty sensors detection or malicious data injections detection. Therefore, there is a need for a surveythat analyses the

achievements and shortcomings of the work targeted to maliciousdata injections and reviews the state-of-the art techniques proposed fornon-malicious data compromise and evaluates their suitability to this problem.

2. Literature Survey

Wireless sensor Networks (WSNs) [1] are helpless and malicious to trade of by physically or remotely, with conceivably destroying impacts. At the point when sensor networks are utilized to detect the event of occasions, for example, fires, interlopers, then again heart attacks, malicious information may be infused to make fake events and hence trigger a not aimed reaction or to cover the event of real occasions. Creator proposes a novel calculation to distinguish malicious information infusions and assemble estimation assumes that are impervious to a few traded off sensors notwithstanding when they conspire in the attack [1]. Author proposes a technique to implement this algorithm in various application settings and assess its outcomes on three diverse datasets peaked from unique WSN arrangements. This leads us to recognize distinctive exchanges in the configuration of such algorithms and how they are impacted by the application context.

In [2], author 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. 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.

Usefulness of a Wireless Sensor Network for detecting numerous event sources is explore in [3] by utilizing binary information. Sensor node has normal nature, sensing can be disturbed which results in invalid observations. So it is necessary to use of event recognizing algorithm in Wireless Sensor Networks (WSNs) identify fault tolerant nature to track malicious nodes. This paper implements a less difficulty, distributed, real-time algorithm which uses the binary analysis of the sensors instead of datasets to identify, localize and tracking of events.

Author of [4] shows a software confirmation plan for dynamic information integrity based on information limit integrity. It naturally changes the source code and installs information guard to monitor runtime program information. An information guard is not retainable if it is damaged by an attacker, regardless of the possibility that the attacker completely handles the structure later. The damage of any information guard at runtime can be remotely distinguished. Damage either shows a software attack or a bug in the software which requires quick consideration.

Proposes reconciliation of framework observing modules and intrusion detection modules in the connection of WSNs. They propose an Extended Kalman Filter (EKF) based system to identify false infused information. In specific, by observing natures of its neighbors and utilizing EKF to expect their future states (real in-network collected values), every node goes for setting up an ordinary scope of the neighbor's future transferred collected values. This undertaking is trying due to possibly large packet loss rate, harsh scenario, detecting vulnerability, so forth.

Technique in [6] show another class of attacks, named false data infusion attacks, against state calculation in electric energy matrices. They illustrate that an attacker can misuse the setup of an energy mechanism to dispatch such attacks to viably present discretionary errors within some state variables while bypassing previous methods for terrible calculation recognition. What's more, they take two sensible attack circumstances, in that the attacker is forced to some particular meters (in light of the fact that of the physical security of the meters), then again restricted in the benefits needed to deal meters.

In paper [7] proposes an exceedingly versatile cluster-based hierarchical trust administration convention for wireless sensor networks (WSNs) to adequately manage self-centered or malicious nodes. Not at all like former work, have they considered multidimensional trust features decided from interaction and social networks to survey the general trust of a sensor node. By system for a new possibility model, they illustrate a heterogeneous WSN containing a broad numerous sensor nodes with immensely particular social and Quality of service (QoS) natures with the aim to yield "ground truth" node status.

In paper [8], accurate analysis and decision-making depends on the nature of WSN data and in addition on the extra data and context. Raw observations from sensor node, in any case, might have low data quality and reliability because of restricted WSN assets and cruel sending situations. This article addresses the nature of WSN data concentrating on anomaly detection. These are characterized as perceptions that don't fit in with the normal conduct of the data. The created technique depends on time-arrangement investigation and geostatistics.

In paper [9], while wireless sensor network are ended up being a flexible tool, a hefty portion of the applications in which they are executed have delicate data. At the end of the day, security is crucial in any of these applications. Once a sensor hub has been traded off, the security of the system corrupts rapidly if there are not measures brought to manage this occasion.

In paper [10], author created the outline, deployment and assessment of TinyECC, a configurable library for ECC operations in remote sensor systems. The essential target of TinyECC is to give a prepared to-utilize, openly accessible programming package for ECC based PKC operations which may be adaptably arranged and coordinated within sensor network applications. TinyECC gives various improvement switches, which can turn particular enhancements on or off in view of developer's needs.

Table 1: Comparative Analysis

Paper	Problem	Techniques	Advantage	Disadvantage/Future Scope	Results
Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection (2012)	deal with selfish or malicious nodes	probability model utilizing stochastic Petri nets technique	A hierarchical dynamic trust management protocol with social trust and QoS trust	devising and validating a decentralized trust management scheme for autonomous WSNs without base stations	trust-based geographic routing protocol performs close to the ideal performance of flooding-based routing in delivery ratio and message delay without sacrificing much in message overhead compared with traditional geographic routing protocols which do not use trust
A Trust-Based Framework for Fault-Tolerant Data Aggregation in Wireless Multimedia Sensor Networks (2012)	Worked in noisy and unattended environments	data aggregation, information trust, and fault tolerance to enhance the correctness and trustworthiness of collected information	significantly decrease the impact of erroneous data andprovide measurable trustworthiness for aggregated data.	More data intrusion model and design more perfect fault tolerantand intrusion-tolerant mechanism.	validate and efficient framework, which significantly improve the quality of multimedia information as well as more precisely evaluate the trustworthiness of collected information
Online Anomaly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring (2014)	Faulty Measurements in healthcare monitoring	Haar wavelet decomposition, non-seasonal Holt–Winters forecasting, and the Hampel filter for spatial analysis, and on for temporal analysis	suitable for online detection and isolation for faulty or maliciously injected measurements with low computational complexity and storage requirement.	This system can be applied to online anomaly detection using the Shimmer platinum development kit, Also reduce the energy wastage	Efficiency and reliability, by identifying faulty measurements and reducing the number of false alarms.
DataGuard: Dynamic data attestation in wireless sensor networks (2013)	ensuring software integrity in wireless sensor networks	a software attestation scheme for dynamic data integrity based on data boundary integrity	it does not rely on any additional hardware support, making it suitable for low cost sensor nodes. Second, it introduces minimal communication cost and has adjustable runtime memory overhead.	it does not support fine-grained data protection, such as protect array element individually	The prototype implementation and the experiments on TelosB motes show that the proposed technique is both effective and efficient for sensor networks.
Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation (2016)	centralized detection of a binary event in the presence of falsifiable sensor nodes	Distributed Binary Event Detection	Working in less energy bandwidth	System can be enhanced with a general (non-linear) optimal combining strategy at the FC and study attackers that do not know the true state of the target	Based on a simple linear weight combining rule at the FC and adopting the modified deflection coefficient

3. Research Directions

Novel research in the event detection WSN field is desirable to:

- Measure the theoretical properties of event detection WSN and study, how these properties are usedin sensing and communication devices
- Establish better model or tools to improve the security of sensor devices
- Invent new network protocols that relate to the event detection of real world environments
- Test the individual solutions of each new approach on real time platforms in real settings, and make novel solutions into a complete malicious data injection detection systems.

Even though wireless sensor network and event detection has great demand, the development related to this areahas not that much of attended.Here some study suggest that, researcher can use some artificial intelligence and neural network related techniques to make sensor nodes smarter. This will help to reduce the burden of traditional event detection approaches in which malicious data injection detection is major challenge. Also expand such type of methods, which makes sensor smarter and can be able to take the decision of disaster cure and prevent.

4. Propose System

This system proposes a new algorithm to recognize malicious data injections and construct measurement estimates that are resistant to several compromised sensors even when they collude in the attack. We also ranges for the event detection. If and only if number of sensor observations matching the given range only that time event will be detected. This will helps to enhance the security.

In propose system, initially sensors read the dataset and then select the dataset for estimation. The estimation procedure comprise of estimating the other nodes values, through which a trust based system can be set up between the nodes and the system to know which node has a possibility of being messed with and the likelihood of being a malicious node. For each new estimation collect by a sensor, dissimilar pairwise estimates are intended through the estimation models. Now we aggregate them into a final estimate and permit us to detect the presence of malicious data injections. Each reported estimation has an evaluation of the observed value from the estimate aggregation step. To recognize data injections in estimation, we look at the two utilizing a similarity metric that must be steady with the event detection model. Consequently, two signals that are similar according to the metric must also have similar effects on the event detection and vice-versa. At the point when the similarity check fails for a sensor, the sensor may have been compromised by malicious data. Though, in few cases the similarity check could also fail on real sensors, due to the wrong methodology was selected or due to the estimation was disturbed by compromised sensors.

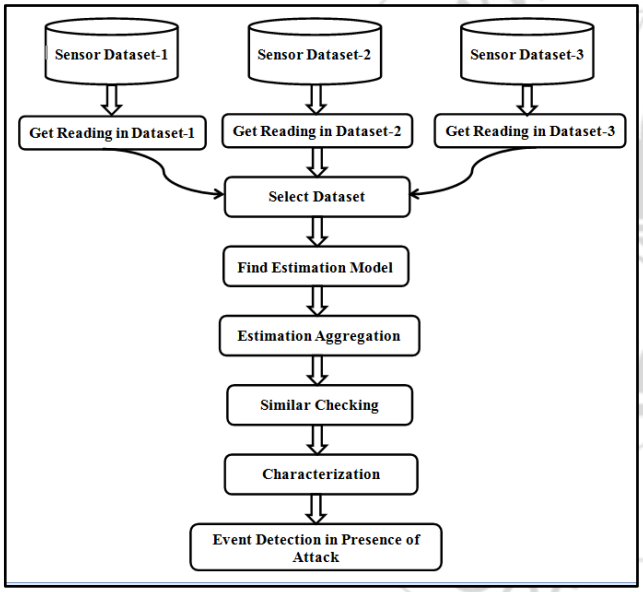

Figure 1: System Architecture

5. Conclusion

Malicious data injections are the challenging issue in event detection WSNs. This survey reviewed recent techniques. This techniques can detect malicious data injections by defining an expectedbehavior. After this detect the deviations from it.We discussed the different techniques, how are implemented, what are the advantage and disadvantage and final conclude with their results.

6. Acknowledgment

The authors are thankful to the publishers, researchers for making their resources available and also appreciate the comments and suggestions obtained from the reviewers, which are useful to improve the quality of paper.

References

[1] Vittorio P. Illiano and Emil C. Lupu, "Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks", IEEE Transactions on Network and service management, Vol. 12, NO. 3, September 2015.
[2] Miss. Rohini Diwase, Prof. Dr. Srinivasa Narasimha Kini, "A Survey on Problems Faced in Identification of Malicious Data Insertion in Wireless Sensor Networks and Rectification of It", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064
[3] Miss. Rohini Diwase, Prof. Dr. Srinivasa Narasimha Kini, "Event Detection in Wireless Sensor Network with Malicious Data Detection Using Binary Data", Fifth Post Graduate Conference of computer Engineering, CPGCON 2016
[4] D. Zhang and D. Liu, "DataGuard: Dynamic data attestation in wireless sensor networks", in Proc. IEEE/IFIP Int. Conf. DSN, 2010, pp. 261270.
[5] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks", Syst. J., vol. 7, no. 1, pp. 1325, Mar. 2013.
[6] Y. Liu, P. Ning, andM. K. Reiter, "False data injection attacks against state estimation in electric power grids", Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 2132, May 2011.
[7] F. Bao, I.-R.Chen, M. Chang, and J.-H.Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", IEEE Trans. Netw. Service Manage, vol. 9, no. 2, pp. 169183, Jun. 2012.
[8] Y. Zhang et al., "Statistics-based outlier detection for wireless sensor networks", Int. J. Geogr. Inf. Sci., vol. 26, no. 8, pp. 1373-1392, 2012.
[9] M. Mathews, M. Song, S. Shetty, and R. McKenzie, "Detecting compromised nodes in wireless sensor networks", in Proc. SNPD, 2007, vol. 1, pp. 273278. 106
[10] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks", in Proc. IPSN, 2008, pp. 245256.