International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Malicious Data Detection Using Binary Data with Event Detection in Wireless Sensor Network

Surendra Kumar, **Prof. Gurudev B. Sawarkar**
Department of Computer Science and Engineering, V. M. Institute of Engineering & Technology, Nagpur, Maharashtra, India

ABSTRACT

Wireless sensor networks (WSNs) is simpler to get to either physically or remotely. In this system, malicious data is injected on sensor hubs to create fake occasions. Existing frameworks distinguish the malicious data injections on hubs. This framework needs a dataset which is utilized to distinguish the occasions. This framework lessens the execution and effectiveness of the occasion discovery prepare. To conquer these confinements, this paper investigates the handiness of a Wireless Sensor Network for identifying various occasion sources by using paired data. Sensor hub has typical nature, detecting can be irritated which brings about invalid perceptions. So it is important to utilization of occasion perceiving calculation in Wireless Sensor Networks (WSNs) distinguish blame tolerant nature to track malicious hubs. This paper executes a less trouble, circulated, continuous calculation which utilizes the paired examination of the sensors rather than datasets to recognize, confine and following of occasions. Exploratory results demonstrate that the proposed calculation enhances following precision in nearness of commotion and issues.

Keywords : Wireless sensor networks, Malicious node, Event detection, Fault tolerant, Binary data.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) can give effective moreover, fiscally reasonable responses for a huge accumulation of employments, for example, wellbeing watching, logical data gathering, condition checking, and military operations. Obviously, sensor centers in these applications are anything but difficult to trade off and can imbue self-emphatically contorted qualities into the frameworks. WSNs are routinely used to recognize occasions occurring in the physical range transversely over varying applications, for example, military observation, prosperity, and condition (e.g., spring of gushing lava) watching. Despite the way that these applications have contrasting assignment, they all gather sensor estimations and translate them to perceive events, i.e., legitimate states of intrigue took after by a mending response. Such response may have imperative outcomes and cost. Along these lines, the estimations making a beeline for the event revelation change into an essential asset for secure.

Right when the estimations are somehow supplanted or changed by an attacker, they supervise malicious data mixtures. The aggressor may utilize the implanted data to move an occasion reaction, for example, flight by temperance of flame, when occasion is not happened, or cover the event of a true blue occasion, for example, the trigger for an intrusion alert. Arranged means for taking control on the estimations are likely. A broad number of the reviews in the securing in order to compose address physical and framework layer perils the reliability of the estimations amidst their transmission. However strikes may trade off the estimations even some time starting late they are transported. For example, an aggressor may modify with a sensor in the region and stack programming that reports wrong estimations. Probability is that the attacker controls condition through using for case a lightweight to trigger a fire alarm.

WSNs are oftentimes used to recognize events occurring in the physical space across over different applications, for instance, military perception, prosperity, and condition checking. In spite of the way

that these applications have differing assignments, they all accumulate sensor estimations and make an interpretation of them to perceive events, i.e., particular conditions of intrigue took after by a therapeutic response.

Such response may have basic results and cost. Along these lines, the estimations provoking the event acknowledgment transform into a fundamental resource for secure. Exactly when the estimations are somehow supplanted or modified by an attacker, we oversee malicious data imbuements. The attacker may make usage of the implanted data to bring out an event response, for instance, flight by virtue of fire, when no event has happened, or cover the occasion of a honest to goodness event, for instance, the trigger for an interference alarm. Unmistakable means for overseeing the estimations are possible.

Remote sensor networks (WSNs) are regularly used to distinguish occasions happening in the physical space applications. Applications have different assignments, for example, accumulate sensor estimation and characterize them to recognize occasions. Counts are prompts the occasion discovery and develop into a crucial asset to ensure. On the off chance that assailant can supplanted or changed the estimations, then we manage malicious data mixtures. Proposed calculation perceives malicious data imbuements and makes computation that is impenetrable to many traded off sensors regardless of the possibility that they confront the assault. Moreover proposed procedure executes this calculation in different application settings and registers its results on three different datasets drawn from one of a kind WSN actualizes. Remote sensor networks (WSNs) every now and again used to occasions occurring in the physical space applications have particular assignments assemble sensor estimations and decipher them to perceive occasions and that estimations provoking the event distinguishing proof, transform into an essential resource for secure. Exactly when the estimations are by some methods supplanted or balanced by an attacker, we oversee malicious data injections. We propose another computation to perceive malicious data mixtures and manufacture estimation evaluates that are impenetrable to a couple exchanged off sensors despite when they plot in the assault.

We in like manner propose a rationality to actualize these calculations in different application settings and evaluate its results on three assorted datasets drawn from unmistakable WSN game plans.

II. RELATED WORK

Wireless sensor Networks (WSNs) [1] are vulnerable and malicious to exchange of by physically or remotely, with possibly crushing effects. Right when sensor networks are used to recognize the occasion of events, for instance, fires, intruders, on the other hand heart assaults, malicious data might be imbued to make fake occasions and thus trigger a not pointed response or to cover the occasion of genuine events. Maker proposes a novel figuring to recognize malicious data implantation and a mass estimation expect that are impenetrable to a couple exchanged off sensors despite when they scheme in the assault [1].

Creator proposes a procedure to actualize this calculation in different application settings and survey its results on three assorted datasets topped from one of a kind WSN courses of action. This leads us to perceive unmistakable trades in the setup of such calculations and how they are affected by the application setting. Creator [2] demonstrates a product affirmation get ready for dynamic data uprightness in light of data point of confinement trustworthiness. It normally changes the source code and introduces data protect to screen runtime program data. A data monitor is not retainable on the off chance that it is harmed by an aggressor, paying little mind to the likelihood that the assailant totally handles the structure later. The harm of any data watch at runtime can be remotely recognized. Harm either demonstrates a product assault or a bug in the product which requires fast thought. The benefits of the proposed affirmation plan are as indicated by the going with. Regardless, it doesn't base upon any additional equipment support, making it fitting for less esteem sensor hubs. Second, it presents inconsequential correspondence esteem and has adaptable runtime memory overhead. Third, it works paying little mind to the likelihood that sensor hubs utilize particular equipment stages, the length of they run the comparative programming. The model sending and the tests on TelosB bits show that the proposed technique is both reasonable and successful for sensor networks.

Creator [3] proposes compromise of structure watching modules and interruption location modules in the association of WSNs. They propose an Extended Kalman Filter (EKF) based framework to distinguish false mixed data. In particular, by watching natures of its neighbors and using EKF to expect their future states (genuine in-system gathered qualities), each hub goes for setting up a conventional extent of the neighbours' future exchanged gathered qualities. This endeavor is attempting because of conceivably extensive bundle misfortune rate, unforgiving situation, distinguishing defencelessness, so forward. They lay out how to use EKF to convey this issue to make fruitful neighbourhood recognition approach. Using specific collections capacities (typical, aggregate, max, and min), they demonstrate to get a hypothetical edge. They help execute a calculation of total Summation (CUSUM) and Generalized Likelihood Ratio (GLR) to develop distinguishing proof affectability.

Creators [4] demonstrate another class of assaults, named false data mixture assaults, against state count in electric vitality frameworks. They show that an aggressor can abuse the setup of a vitality system to dispatch such assaults to feasibly display optional blunders inside some state factors while bypassing past techniques for unpleasant count acknowledgment. Also, they take two sensible assault conditions, in that the aggressor is compelled to some specific meters (in light of the way that of the physical security of the meters), of course limited in the advantages expected to arrangement meters. They display that the aggressor may professionally and competently create assault vectors in both conditions, which can't just adjust the results of state estimation, besides modify the results in subjective way.

Creator [5] proposes an exceedingly flexible group based progressive trust organization invention for remote sensor networks (WSNs) to satisfactorily oversee narcissistic or malicious hubs. Not in the slightest degree like previous work, have they considered multidimensional trust highlights chosen from cooperation and informal communities to study the general trust of a sensor hub. By framework for another probability demonstrate, they represent a heterogeneous WSN containing a wide various sensor hubs with enormously specific social and Quality of administration (QoS) natures with the mean to yield "ground truth" hub status. This presents as a purpose behind contrasting so as with endure their convention execution at subjective trust made as a result of convention execution at runtime against target trust picked up from genuine hub status.

In paper [6], exact investigation and decision making relies on upon the way of WSN data and what's more on the additional data and setting. Crude perceptions from sensor hub, regardless, may have low data quality and unwavering quality as a result of confined WSN resources and merciless sending circumstances. This article addresses the way of WSN data focusing on irregularity discovery. These are described as discernments that don't fit in with the ordinary lead of the data. The made system relies on upon time-game plan examination and geostatistics.

In paper [7], while remote sensor systems are wound up being an adaptable instrument, a weighty segment of the applications in which they are executed have sensitive data. By the day's end, security is pivotal in an any of these applications. Once a sensor center point has been exchanged off, the security of the framework adulterates quickly if there are not measures conveyed to deal with this event. There have been various systems analysed to deal with the issue. In this paper, we explore an inconsistency based intrusion area framework to perceive exchanged off center points in remote sensor frameworks. A calculation to perceive the bargained sensor hub has been delivered.

In paper [8], creator made the layout, arrangement and appraisal of TinyECC, a configurable library for ECC operations in remote sensor frameworks. The fundamental focus of TinyECC is to give an arranged to-use, straightforwardly open programming bundle for ECC-based PKC operations which might be adaptably organized and facilitated inside sensor arrange applications. TinyECC gives different change switches, which can turn specific improvements on or off in perspective of designer's needs.

In paper [9], creator proposes a lightweight strategy for online recognizable proof of flawed estimations by examining the data assembled from remedial remote body zone frameworks. The proposed framework performs progressive data examination using a PDA as a base station, and considers the constrained resources of the propelled cell, for instance, get ready power and limit restrain. The major target is to raise cautions

exactly when patients enter in an emergency situation, and to hurl false alerts initiated by defective estimations or ill-behaved sensors. The proposed system relies on upon the Haar wavelet disintegration, non-regular Holt Winters determining, and the Hampel channel for spatial investigation, and on for worldly examination. We will likely decrease false cautions coming to fruition in light of hazardous estimations and to lessen pointless human administrations intervention.

III. IMPLEMENTATION DETAILS

A. System Overview

Proposed System is functioning as takes after:

1) Here first send the hubs in the specific zone field. These hubs are static and client can send the same number of as he needs.
2) Here the client will convey the Event source. This occasion source we need to screen. This is our system of hubs and where the real fire is called occasion source. So occasion source is the area of occasion set.
3) There will be sure scope of each sensor called as REGION OF COVERAGE. So it will demonstrate just the area of that sensor hub.
4) Now, we need to choose a pioneer in an area of membership utilizing conveyed adaptation to non-critical failure calculation as given underneath.

ROS = 2 ROC
ROS = region of subscription
ROC = region of coverage
5) For each ROS there will be one pioneer as it were. Furthermore, ROS (Region of subscription) is constantly more noteworthy than ROC (Region of coverage)
6) Here we will utilize another method for disturbing sensors. Here subsequent to putting occasion source, if the occasion source is in locale of scope of the sensor then it will get frightened. At that point each frightened sensor will deliver +1 esteem and each non-frightened sensor will create - 1 esteem. Just the locale of scope of LEADER hub will demonstrate the qualities as appeared in above picture. Each sensor will deliver values however just the ROC of pioneer hub will demonstrate values.

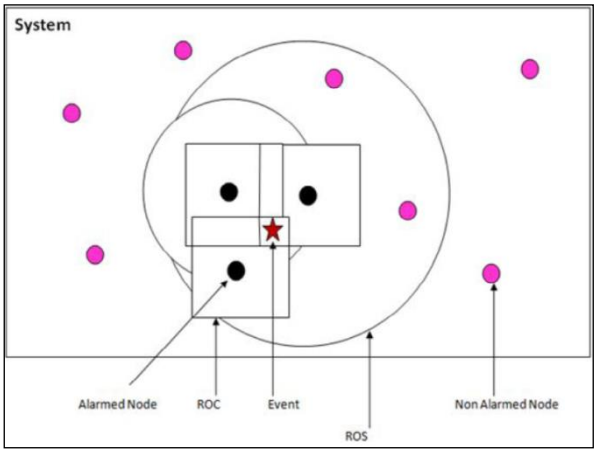

Fig. 1: System Architecture

B. Mathematical Model

System S is represented as
S= {Input, Process, Output}

- Input: Parameters of all node
- Process:

1. Deploy Set of all nodes N= {n1, n2, ...,ni} Where, N is the set of all nodes deployed in the network.
2. Enter source event S Source node is attacker
3. Detect Alarmed nodes A= {a1, a2, ..., an} Where A is a set of alarmed node, which are present into region of interest of source events.
4. Detect Non Alarmed nodes.

NA= {na1, na2... nan} Where NA is a set of non-alarmed node, which are not present into region of interest of source events.

5. Identification of region of subscription (ROS)

ROS= 2ROC
Where, region of coverage

6. Leader Selection

For leader selection, system applies leader election protocol. Leader node is an Alarm nodes which are exist in a ROC and whose Fn>0. Where, Fn is a random function of nodes, which provide binary values to the nodes.

7. Identify all paths from source to destination and select shortest one. P= {p1, p2... pn} Where, P is a set of all paths from Source to destination.
8. Detection of faulty nodes F= {f1, f2... fn} Where, F is a set of all faulty nodes, detected by leader.

Output: Data sending and source event localization.

C. Algorithm

Algorithm 1 D-FTLEP: Distributed Fault Tolerant Leader Election Protocol

Input: Set of neighboring alarmed sensor nodes A.

Output: Elected leader status.

1: All alarmed sensors broadcast an ALARM message.
2: Node n calculates the function Fn using the received ALARM messages from its neighbors.
3: If Fn>0 then continue with next step else STOP.
4: Wait for a period h (1/Fn).
5: If during the waiting period a LEADER message with value f Fn is received STOP.
6: Broadcast LEADER message with value Fn and assume leadership role.

F_n is the summation of each sensor esteem in a sensors locale of scope.

F_n= estimation of sensors which is in the area of scope of nth hub.

We need to compute this incentive for every single hub. And after that make a sensor hub as pioneer whose F_n esteem is higher than others.

In the event that F_n>0 it implies no less than one source is identified. On the off chance that the estimations of two sensors are a similar then pioneer will be one who is nearer to the occasion source. Clearly the occasion source ought to be available in chosen pioneers area of scope.

Algorithm 2 Scoring Matrix Construction

Input: [Xn, Yn, bn] for sensor nodes n = 1, ...,Nl2ROSl

Output: Scoring matrix Ll

1: Ll0
2: for all cells M1 l (i, j) 2 Gldo
3: for all sensor nodes n that have cell M1 l(i, j) to ROC and do
4: Ll(i, j) Ll(i, j) + bn
5: end for
6: end for

IV. CONCLUSION AND FUTURE SCOPE

In this framework our fixation is on recognizing malicious data mixtures in occasion recognition WSNs, in particular when conspiracy inside traded off sensors happens. Existing frameworks recognize the malicious data injections on hubs. We have proposed a calculation which might be tweaked and used in different applications and for different sorts of occasions. For head choice we utilize pioneer decision convention. For occasion discovery we utilized Fault tolerant restriction and following convention. We distinguish the briefest way for secure data sending from source to goal. To assess the framework execution, we utilize JUNG test system, which demonstrate that the proposed framework is productive for source occasion identification.

V. 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]. D. Zhang and D. Liu, ”DataGuard: Dynamic data attestation in wireless sensor networks”, in Proc. IEEE/IFIP Int. Conf. DSN, 2010, pp. 261270.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. M. Mathews, M. Song, S. Shetty, and R. McKenzie, ”Detecting compromised nodes in wireless sensor networks”, in Proc. SNPD, 2007, vol. 1, pp. 273278.

[8]. A. Liu and P. Ning, ”TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks”, in Proc. IPSN, 2008, pp. 245256.

[9]. O. Salem, Y. Liu, A. Mehaoua, and R. Boutaba, ”Online anomaly detection in wireless body area networks for reliable healthcare monitoring”, J. Biomed. Health Informat., vol. 18, no. 5, pp. 15411551, Sep. 2014.

[10]. 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. 8594. 47

[11]. F. Liu, X. Cheng, and D. Chen, ”Insider attacker detection in wireless sensor networks”, in Proc. 26th IEEE INFOCOM, 2007, pp. 19731945.

[12]. 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. inProc. 7th ACM Int. Symp. Mobile Ad Hoc Netw.Comput., 2006, pp. 356367.

[13]. S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, “Quarter sphere based distributed anomaly detection in wireless sensor networks,” in Proc. IEEE ICC, 2007, pp. 3864–3869.

[14]. V. Chatzigiannakis and S. Papavassiliou, “Diagnosing anomalies and identifying faulty nodes in sensor networks,” IEEE Sensors J., vol. 7, no. 5, pp. 637–645, May 2007.

[15]. S. Rajasegarar, J. C. Bezdek, C. Leckie, and M. Palaniswami, “Elliptical anomalies in wireless sensor networks,” Trans. Sensor Netw., vol. 6, no. 1, pp. 1550– 579, 2009.

[16]. A. B. Sharma, L. Golubchik, R. Govindan, “Sensor faults: Detection methods and prevalence in real-world datasets,” Trans. Sensor Netw., vol. 6, no. 3, pp. 23–61, 2010.

[17]. Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 21–32, May 2011.

[18]. Q. Zhang, T. Yu, and P. Ning, “A framework for identifying compromised nodes in wireless sensor networks,” Trans. Inf. Syst. Secur., vol. 11, no. 3, pp. 1–37, Mar. 2008.

[19]. C. V. Hinds, “Efficient detection of compromised nodes in a wireless sensor network,” in Proc. SpringSim, 2009, Art ID. 95.

[20]. W. Zhang, S. K. Das, and Y. Yonghe, “A trust based framework for secure data aggregation in wireless sensor networks,” in Proc. 3rd Annu. IEEE SECON, 2006, pp. 60–69.

[21]. 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. 169–183, Jun. 2012.

[22]. B. Przydatek, D. X. Song, and A. Perrig, “SIA: Secure information aggregation in sensor networks,” in Proc. SenSys, 2003, pp. 255–265.

[23]. S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks: Filtering out the attacker’s impact,” IEEE Trans. Inf. Forensics Security, 2014, pp. 681–694.

[24]. Y. Sun, H. Luo, and S. K. Das, “A trust-based framework for faulttolerant data aggregation in wireless multimedia sensor networks,” IEEE Trans. Dependable Security Comput., vol. 9, no. 6, pp. 785–797, Nov./Dec. 2012.