ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Use of binary data for malicious data detection and event detection in Wireless Sensor Network

Rohini Divase[1], Prof. Dr. Srinivasa Narasimha Kini[2]

M.E Student, Department of Computer Engineering, JSPM College of Engineering, Hadapsar, Pune, India

Assistant Professor, Department of Computer Engineering, JSPM College of Engineering, Hadapsar, Pune, India

ABSTRACT: Wireless Sensor Networks (WSNs) can be faulty remotely as well as physically. For creating fake events wrong data can be inserted on sensor node in this type of network. Present systems are able to find the insertion of faulty data on the nodes only. For finding the events this system must have a dataset. This will reduce the performance and efficiency of the event detection process. To solve this issue, this paper explores the utilization of a WSN for finding various event sources by making use of binary data. Sensing can be disturbed which results in invalid observation due to the simple nature of sensor node. So it is must that, used event tracking algorithm in WSNs finds fault tolerant behavior to track malicious nodes. This paper implements algorithm which makes use of the binary observations of the sensors in the place of dataset for finding, localize as well as tracking of events which is low-complexity, distributed, real time. Test outcomes shows that the proposed algorithm maximizes tracking accuracy in presence of noise as well as faults.

KEYWORDS: Wireless sensor networks, malicious node, Event detection, Fault tolerant, binary data.

I. Introduction

Wireless Sensor Networks (WSNs) is able to provide effective and finically suitable answers for a significant group of uses, for example, health observing, scientific data gathering, environment checking, and military operations. Defiantly, sensor hubs in above stated applications can be changed and can add self-assertively distorted qualities into the systems. For finding events going on in the physical space WNSs are commonly used such as, military surveillance, wellbeing, and environment (e.g., volcano) monitoring. However in the manner that these applications have different task, they all gather sensor estimations as well as decode them to find the occasion i.e. specific conditions of interest took after healing reaction. Response like this can have noteworthy outcome as well as cost. In this manner, the estimations heading to the occasion discovery transform into a fundamental resource for secure.

When the estimations are some way or another supplanted or changed by an assailant, they oversee malicious injections of data.

The hacker can use the introduced information forcreating an event response, for instance, flight depending on fire, when event has not done, or shroud the occasion of a bona fide event, such as, the presence for an interruption caution. Assorted means for taking control on the evaluations are possible. Large number of the studies in the securing so as to write solve physical and system layer dangers the trustworthiness of the guess in the midst of their transmission. However attacker may be exchange off the estimations even some time as they are forwarded. Such as, an attacker may align with a sensor in the field and denotes programming that reports false estimations. Likelihood is that the attacker controls environment by making use of for case a lighter to trigger a flame alert.

The use of WSNs is mainly for differentiation of happenings in the given physical area crosswise for different applications. Such as military observation, wellbeing, and environment checking. Regardless of the fact that these applications have different works, they all collect sensor estimations and send them to identify occasions, i.e., specific states of interest took after by a medicinal reaction. This type of reaction can have major consequences and cost. In

DOI: 10.15680/IJIRCCE.2016. 0406360

such manner, the estimations prompting the event recognition turn into a fundamental asset to save. Exactly when the estimations are somehow supplanted or changed by an attacker, we oversee faulty information injections. The attacker may make use of the implanted information to evoke an event response, for instance, departure on account of flame, when no occasion has happened, or cover the event of a genuine occasion, for example, the trigger for an interruption alert. Particular means for getting control over the estimations are possible.

Wireless sensor networks (WSNs) commonlyutilized for detection of events happening in the physical space applications have numerous tasks gather sensor measurements and observes them to find events and that measurements leading to the event detection, has been a major resource to secure. When the measurements are replaced or altered by an attacker, we deal with malicious data injections. We propose a novel algorithm to identify malicious data injections and build measurement estimates that are resistant to several compromised sensors even when they conspire in the attack. We also propose a processor applying this algorithm in variousapplications on texts and calculate its outcomes on three totally different datasets drawn from distinct WSN deployments.

In this paper we study about the related work done on the feature selection techniques in section II, the implementation details in section III where we see the system architecture, modules description, mathematical models, algorithms and experimental setup. In section IV we discuss about the expected results and at last we provide a conclusion in section V.

II. Related work

Wireless sensor Networks (WSNs) [1] are helpless and can be maliciously given up, by physically or remotely, with probably deleting impacts. When sensor networks are utilized for detecting the event of happening, for example, fires, interlopers, then again heart attacks, wrong information can be inserted to make fake events and hence trigger an undesired reaction or to cover the event of real occasions. Authors has given a new computation to differentiate malicious injections of data and assemble estimation assumes that are impervious to some traded off sensors However, when they plot in the attack [1]. Author implemented a method to apply this algorithm in number of application settings and assess its results on three different datasets taken from various WSN arrangements. This leads us to recognize distinctive tradeoffs in the configuration of such algorithms and how they are observed by the application perspective.

Author [2] given a software confirmation plan for dynamic data integrity depending on data limit integrity. It modify the source code and installs data guards to track runtime program data. A data guard is not recoverable once it is altered by a hacker, indifferent of the possibility that the attacker completely controls the structure later. The corruption of any data guard at runtime can be remotely distinguished. A corruption shows a software attack or a bug in the software that wants quick taken in account. The pros of the proposed plan are according to the accompanying. In any case, it doesn't depend on any external hardware support, which making it preferable for low cost sensor nodes. Second, it presents insignificant correspondence cost and has customizable runtime memory overhead. Third, it does not work depending on any of the possibility that sensor nodes utilize different hardware platforms, the length of they run the similar software. The model development as well as the tests on TelosB bits exhibit that the given method is suitable as well as efficient for sensor networks.

Author [3] given reconciliation of system observing modules and intrusion detection modules in the connection of WSNs. They introduced an Extended Kalman Filter (EKF) depended on framework to search false injected data. In particular, by observing working of its neighbors and utilizing EKF to guess their future states (real in-network collected values), every node goes for setting up a normal scope of the neighbors' future transmitted aggregated values. This attempt is trying because of possibly high packet loss rate, harsh environment, detecting vulnerability, so forth. They layout, how to use EKF to get this issue to make successful local detection method. By making use of specific aggregations functions (normal, total, max, and min), they proved how to get a theoretical threshold. They help apply an algorithm of cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) to extend identification sensitivity.

DOI: 10.15680/IJIRCCE.2016. 0406360

Authors [4] show another class of attacks, called false data injection attacks, against state estimation in electric power matrices. They illustrate that an attacker can misuse the setup of a power system to dispatch such attacks to viably introduce arbitrary errors into certain state variables while bypassing existing techniques for terrible measurement recognition. What's more, they take two sensible attack circumstances, in which the attacker is either constrained to some particular meters (in light of the fact that of the physical security of the meters), then again restricted in the benefits required to compromise meters. They exhibit that the attacker can systematically and capably develop attack vectors in both circumstances, which can't simply change the results of state estimation, furthermore alter the results in subjective ways.

Author [5] introduced an exceedingly versatile cluster-based hierarchical trust administration convention for wireless sensor networks (WSNs) to adequately manage selfish or malicious nodes. Non like former work, have they taken in account multidimensional trust attributes decided from communication and social networks to survey the general trust of a sensor node. By system for a new probability model, they illustrate a heterogeneous WSN having a broad number of sensor nodes with immensely specific social and Quality of service (QoS) behaviors with the objective to yield "ground truth" node status. This serves as a reason for comparing so as to tolerate their protocol execution at subjective trust made as an outcome of protocol execution at runtime against target trust gained from genuine node status.

In paper [6], accurate analysis and decision-making based on the nature of WSN information as well as on the data and context.Raw studies from sensor node, in all cases, might have low data quality and reliability due to limited WSN assets and cruel forwarding cases. This article takes the nature of WSN information centered on anomaly detection. These are grouped as perceptions that don't fit in with the normal conduct of the information. The method developed depending on time-arrangement investigation and geostatistics.

In paper [7], while wireless sensor network are become a flexible tool, a hefty portion of the applications in which they are executed have sensible information. At last, security is important in every application. Once a sensor hub has been attacked, the security of the system corrupts rapidly if there is no solution present to solve this problem. There are various methods present to solve this above stated problem. In this paper, we study an anomaly-based interruption location system to findattackednodes in remote sensor systems. An algorithm to find the attacked sensor node has been implemented.

In paper [8], author generated the design, implementation, and evaluation of TinyECC, a configurable library for ECC operations in remote sensor framework. The important target of TinyECC is to give a prepared to make use, openly accessible programming package for ECC-based PKC operations which will be adaptably arranged and coordinated into sensor network applications. TinyECC gives number of modified switches, which can turn specific maximization on or off in view of developer’s needs.

In paper [9], author developed a light technique for online identification of faulty measurements by searching the information collected from restorative remote body zone framework. The presentedframeworkdoes successive information examination using a PDA as a base station, and treats the compelled assets of the advanced cell, such as, preparing power and capacity limit. The basic target is to alerts just when patients enter in a crisis case, as well as to remove false alarms triggered by faulty measurements or ill-behaved sensors. The presented techniquebased on the Haar wavelet decomposition, non-seasonalHoltWintersforecasting, and the Hampel filter for spatial analysis, and on for temporal analysis. Our goal is to lessen false alerts coming about because of problematic estimations and to diminish superfluous human services intercession.

III. PROPOSED ALGORITHM

A. *System Overview:*

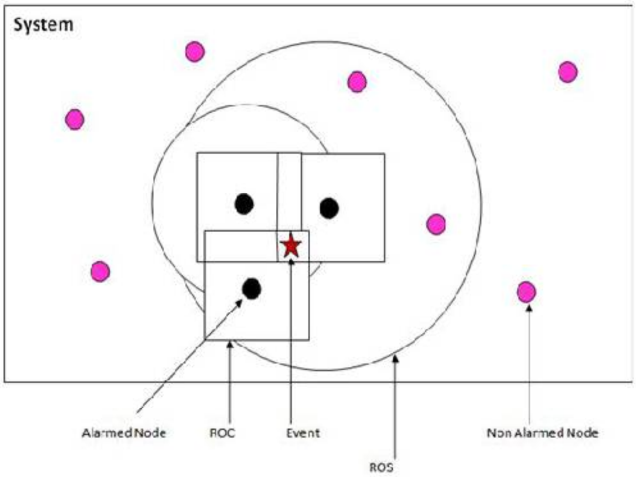

Fig. 1: System Architecture

Proposed System is working as follows:

1. Here first scatter the nodes in the specific area field. These nodes are static and user can deploy as many as he wants.

2. Here the user will send the Event source. This event source we have to observe. This is our network of nodes and the place in which the actual fire is called event source. So event source is the location of event placed.

3. There will be specific range of each sensor called as REGION OF COVERAGE. So it will show only the region of that sensor node.

4. Now, we have to elect a leader in an area of subscription using distributed fault tolerance algorithm as given below.

ROS=2 ROC

ROS=region of subscription
ROC=region of coverage

5. For every ROS there will be one leader And ROS (Region of subscription) is always large than ROC (Region of coverage)

6. Here we will utilize a novel technique for alarming sensors. Here after placing event source, if the event source is in area of coverage of the sensor then it will trigger alarmed. Then each alarmed sensor will produce +1 value and every non-alarmed sensor will produce -1 value. Only the area of coverage of LEADER node will show the values as shown in above image. Every sensor will generates values but only the ROC of leader node will show values.

- Contribution:

In proposed system we have increased the time window increase to 5 which was 3 in the existing system. By increasing the size of time window we can detect an event accurately. We have set min value 21 degree for each sensor node and acceptable difference is 0.50 degree. Every node checks the temperature if the temperature of any node is different for five consecutive reading and if it is in the range then only the system will generate alert of event generation.

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 applyleader 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 noder, 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: D-FTLEP: Distributed Fault Tolerant Leader Election Protocol

Input: Set of neighbouring 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 neighbours.
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.

Fn is the summation of every sensor value in a sensors region of coverage.

Fn= value of sensors which is in the region of coverage of nth node.

We have to calculate this value for each and every node. And then make a sensor node as leader whose Fn value is higher than others.

If Fn>0 it means at least one source is detected. If the values of two sensors are the same then leader will be one who is closer to the event source. Obviously the event source should be present in elected leader's region of coverage.

- Algorithm: 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
```

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. RESULT

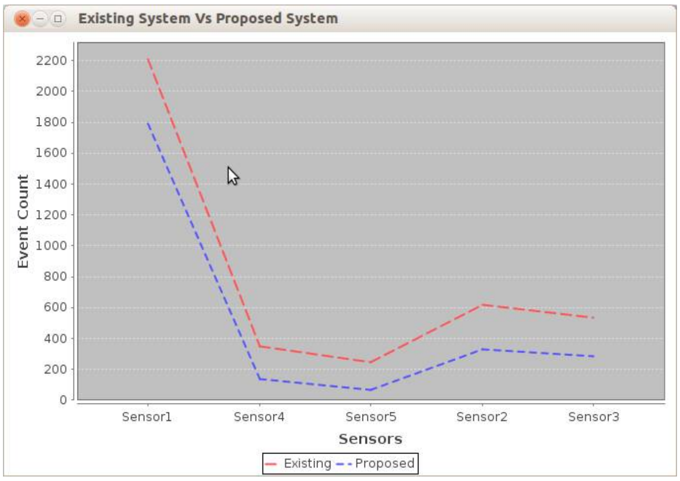

Fig 2: Event Count Comparison Graph

Figure 2 show the comparisonof event count using existing system and using proposed system. As we can see proposed system is able to detect less amount of events as we are giving the limit to the signals. So by this we can detect an event in specific range so the chance of false event will be reduced.

V. CONCLUSION AND FUTURE WORK

Our concentration in proposed system is on finding the malicious data injections while event detection WSNs, specifically when collusion in the faulty sensor nodes occurs. Present framework finds the malicious data insertion on nodes. We proposed an algorithm which will be modify as well as utilized in various applications, also for number of events. We made use of leader selection protocol for head selection. We made use of fault tolerant localization as well as tracking protocol for detecting events. We have found the shortest, preferable path for the secure and safe data transfer from source to destination. We made use of JUNG simulator for evaluation of system performance, which detonated the proposed system efficient for source event detection.

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. 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. 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. 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.