ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

A MALICIOUS AND MISBEHAVIOR NODE DETECTION SCHEME FOR WIRELESS SENSOR NETWORKS

G.Prathiba

Research scholar, Department of Computer Science, Govt. Arts College, Ariyalur, Tamilnadu, India.

P.Selvakumar

Research Supervisor, Asst. Prof. of Computer Science, Govt. Arts College, Ariyalur, Tamilnadu, India.

ABSTRACT

Security is one of the most important issues that have attracted a lot of research and development effort in past few years. In multi-hop wireless ad hoc network link error and malicious packet dropping are two sources for packet losses. Whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop are to be identified, can be known by observing a sequence of packet losses in the network. But in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy because the packet dropping rate in this case is comparable to the channel error rate. therefore to get better the discovery correctness, the correlation flanked by lost packet is recognized. The packet loss information reported by nodes. This technique provides privacy preserving, collusion proof, and incurs low communication and storage overheads. A packet-block based mechanism is also proposed, to reduce the computation overhead of the baseline scheme, which allows one to trade detection accuracy for lower computation complexity.

Keyword Information security, wireless sensor networks, event detection, continuous wavelet transforms

INTRODUCTION

Wireless Sensor Networks (WSNs), motivated by military applications, security has been a major concern. Nowadays, WSNs are popular for IoT applications, such as smart cities, smart grids and healthcare, but security threats could still pose costly and even life-threatening problems. WSNs are by nature exposed to severe vulnerabilities, since they are often physically accessible, unattended, and continuously evolving because of sensors joining and leaving the network. Moreover, the use of security mechanisms such as complex cryptographic mechanisms is restricted because of computational constraints. Thus, the cost of exploiting such vulnerabilities is less a deterrent for malicious activities. In particular, the measurements' integrity may be impaired: we refer to this attack as malicious data injections. Even when common security mechanisms are in place, they cannot prevent some of the attacks. In particular, an attacker can gain control over the WSN by physically tampering with sensor devices or manipulating the environment itself. In several scenarios, these cannot be prevented with proactive security mechanisms. For example, urban traffic sensors may be deliberately biased at the time they are implanted to silence alarms for road accidents. In such luggage, the only denote to offset malicious data injection is discovery from side to side psychiatry of the capacity themselves.

This is possible because of inter-measurements correlation. Correlations exist between measurements of different sensors across the WSN space, which we refer to as spatial correlation. Correlations also exist across the measurements of the same sensor in time, known as temporal correlations, and between multiple monitored phenomena, known as attribute correlations. When spatial correlations are altered, they provide evidence of disagreements between sensors, which are likely to occur when genuine and malicious sensors coexist. Spatial correlation enables detection only if the measurements from a subset of sensors are substantially changed. This assumption is generally valid since the attacker's cost and risk for tampering with measurements of more sensors increases proportionally with their number. On the differing, activist association fails to divulge mean data if the invader tampers with even a solo antenna and apply a level shift between genuine and malicious data. The necessary assumption for the applicability of attribute correlation is that the sensor nodes monitor multiple phenomena, and one of them is not compromised. though, as manifold sensors are linked to the similar antenna node, tamper by it enable the assailant to manage all the monitor phenomenon. The chance of detecting malicious data injections depends on the ability to exploit correlation as well as on the attack's sophistication. We envisage that malicious measurements can be injected with any sophisticated strategy that maximizes the damage to the WSN and minimizes the risk of being detected.

This is possible if compromised nodes collude, i.e., act in concert towards a common goal. The problem becomes even more challenging when events occur in the monitored physical phenomenon. Wildfires are an example of event for temperature monitoringWSNs, while earthquakes are an example of event for seismic WSNs. The effect of events is to transform the measurements correlations, especially when perceived only by a subset of sensors. This real alter in association can be subjugated by a stylish attacker to validate the association filth bring in by mean data. We propose a method for detection of malicious data injections in the presence of sophisticated collusion strategies, based on a cross-scale analysis of the wavelet transform applied to the measurements in the spatial domain. Yet we emphasize that detect anomalies in the capacity is not enough to well offset them. The alteration in the nasty capacity and the precious sensors need to be identified. We refer to this task as characterization. Furthermore, we deal with the diagnosis of the identified anomalies. Indeed, genuine faults may also introduce anomalies, as the measurements from faulty sensors do not correlate with those of healthy ones. This may lead to the wrong conclusion that there was an attack, but by classifying the main characteristics of genuine faults we are able to infer when the anomaly is most likely malicious.

ISSUES AND CHALLENGES

The difficulty becomes more and more multifaceted as the figure of hateful sensors increase. When the attacker's capabilities are sufficiently high, the attacker may correctly reproduce genuine events without triggering detection or make malicious sensors be identified as genuine, and genuine sensors as malicious. The problem becomes even more challenging when events occur in the monitored physical phenomenon. Wildfires are an example of event for temperature monitoring WSNs. Even when common security mechanisms are in place, they cannot prevent some of the attacks. In particular, an attacker can gain control over the WSN by physically tampering with sensor devices or manipulating the environment itself. In several scenarios, these cannot be prevented with proactive security mechanisms.

MOTIVATION

In the proposed to detect generic anomalies rather than deliberate malicious injections, so they are not designed to cope with collusion, this drastically decreases the chances of detection. Moreover, the measurements distribution is assumed homogeneous and this assumption does not hold especially when particular events of interest occur, such as wildfires, earthquakes, pathological conditions, etc. The main idea of trust management techniques is to keep track of a sensor's cooperation in time, assigning it a trust value, which is constantly updated. This can be done by exploiting an expected measurements distribution, or checking if a sensor correctly reports the presence of events of interest. The in order of sensors by means of a low faith assessment is careful less steadfast, and so the bang of wicked data is cheap.

RELATED WORKS

In [1] M. Ameen, J. Liu, and K. Kwak et al presents The use of wireless sensor networks (WSN) in healthcare applications is growing in a fast pace. Numerous applications such as heart rate monitor, blood pressure monitor and endoscopic capsule are already in use. To speak to the rising use of antenna skill in this region, a new field known as wireless body area networks (WBAN or simply BAN) has emerged. As most devices and their applications are wireless in nature, security and privacy concerns are among major areas of concern. Due to direct involvement of humans also increases the sensitivity. Whether the facts gather from patients or persons are obtain with the assent of the being or with no it due to the require by the system, abuse or solitude concern may restrict people from taking advantage of the full benefits from the system. People may not see these devices safe for daily use. present may also option of grave communal strife due to the terror that such plans may be old for monitor and track persons by administration agency or other private organizations. In this papeSensor networks are being used in a wide range of application areas. The major application domains we discuss these issues and analyze in detail the problems and their possible measures. Are, home and office, control and automation, logistics and transportation, environmental monitoring, healthcare, security and surveillance, tourism and leisure, education and training and entertainment. Antenna plans that can be old to monitor being behavior have garner great explore notice in new being. Are, home and office, control and automation, logistics and transportation, environmental monitoring, healthcare, security and surveillance, tourism and leisure, education and training and entertainment.

In [2] M. Li, W. Lou, and K. Ren et al present A new skill for e-healthcare that allow the data of a patient's essential corpse parameter and actions to be calm by tiny wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsettled anxiety, with challenge pending from severe reserve constraint of WBAN plans, and the high be adamant for both security/privacy and practicality/usability. In this article we look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. We discuss various practical issues that need to be taken into account while fulfilling the security and privacy requirements. Relevant solutions in sensor networks and WBANs are surveyed, and their applicability is analyzed. The fast enlargement in wearable medical sensors and wireless communication, wireless corpse region system (WBANs) have emerge as a promising technique that will revolutionalize the way of seeking healthcare, which is often termed e-healthcare. Instead of being measured face-to-face, with WBANs patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, and insurance companies.

In [3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami et al presents Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offer the aptitude to gauge, deduce and appreciate ecological indicator, from delicate ecologies and usual capital to urban environment. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is communal crossways platform in arrange to expand a ordinary in service image (COP).

Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its childhood and is the next radical skill in transform the Internet into a fully included prospect Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly. This document present a shade centric vision for worldwide achievement of Internet of effects. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A blur completion using Aneka, which is base on communication of confidential and community Clouds, is obtainable. We conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community. The after that gesticulate in the era of compute will be exterior the kingdom of the customary desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another.

In [4] C. Karlof and D. Wagner et al presents The routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. We suggest safety goals for direction-finding in antenna network, show how attacks next to ad-hoc and peer-to-peer network can be modified into influential attack next to antenna network, introduce two classes of novel attacks against sensor networks—sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. We explain crippling attack aligned with all of them and propose countermeasures and design consideration. This is the primary such psychoanalysis of safe steering in antenna network. Our focus is on routing security in wireless sensor networks. recent proposal for direction-finding protocol in antenna network optimize for the incomplete capability of the nodes and the function specific nature of the networks, but do not consider security. Although these protocols have not been designed with security as a goal, we feel it is important to analyze their security properties. what time the protector has the liability of unsure of yourself wireless message, incomplete node capability, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol is non-trivial One aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation. In more conventional net Message integrity, authenticity, and confidentiality are handled at a higher layer by an end-to-end security mechanism. In-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. Link layer security mechanisms can help mediate some of the resulting vulnerabilities.

In [5] A. Perrig, J. Stankovic, and D. Wagner et al presents Recent advances in electronics and wireless communication technologies have enabled the development of large-scale wireless sensor networks that consist of many low-powers, low-cost and small-size sensor nodes. Sensor networks hold the promise of facilitating large-scale and real-time data processing in complex environments. Security is critical for many sensor network applications, such as military target tracking and security monitoring. To give safety and loneliness to little antenna nodes is testing, due to the limited capability of sensor nodes in terms of computation, communication, memory/storage, and energy supply. In this article we survey the state of the art in research on sensor network security. Wireless sensor networks have applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. One can envision in the future the deployment of large-scale sensor networks where hundreds and thousands of small sensor nodes form self-organizing wireless networks. Providing security in sensor networks is not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth. in spite of the aforesaid challenge, safety is significant and even dangerous for a lot of application of antenna network, such as armed and mother country safety application. more than a few recent aid to the literature have addressed security and privacy issues in sensor networks. In this article we discuss current and past research activities carried out on sensor network security.

BACKGROUND PROCESS

PACKET DROPPING

pack beat occur while one or spare sachet of data travelling diagonally a computer system fail to reach their goal. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

pack defeat occur when one or extra packets of information travelling across a computer network fail to arrive at their purpose. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. The Transmission Control Protocol (TCP) detects packet loss and performs retransmissions to ensure reliable messaging. envelope trouncing in a TCP link is also old to avoid congestion and therefore produce an deliberately abridged throughput for the link.

ROUTING PROCESS

complex scrutiny is the way of effect the voltages diagonally, and the current from beginning to end, every component in the network. There are many different technique for calculating these values. However, for the most part, the applied technique assumes that the components of the network are all linear. The method described in this editorial is merely appropriate to linear system analysis, but wherever openly affirmed.

PACKET TRANSMISSION

following carrying out the system stage, S enter the pack broadcast stage. S transmits packets to PSD according to the following steps. Before sending out a packet Pi, where i is a sequence number that uniquely identifies Pi, S computes and generates the HLA signatures of ri for node nj, as follows the node has received, and it relays to the next hop on the route. The last hop, i.e., node nK, only forwards Pi to the destination D. As proved in Theorem 4 in Section 4.3, the special structure of the one-way chained encryption construction in (4) dictates that an upstream node on the route cannot get a copy of the HLA signature intended for a downstream node, and thus the construction is resilient to the collusion model defined in Section 3.2. Note that here we consider the verification of the integrity of Pi as an orthogonal problem to that of verifying the tag tji. If the verification of Pi fails, node n1 should also stop forwarding the packet and should mark it accordingly in its proof-of-reception database. **Modules**

- ❖ Set Up Phase
- ❖ Packet Transmission Phase
- ❖ Audit Phase
- ❖ Detection Phase

Set Up Phase

This stage take put right after route PSD is recognized, but previous to any data packet are transmit over the way. In this phase, S decide on a symmetric-key crypto-system encrypt key; decrypt key and K symmetric keys key1; . . . ; key K, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S securely distributes decrypt key and a symmetric key key j to node nj on PSD, for j ¼ 1; . . .;K. Key distribution may be based on the public-key crypto-system such as RSA: S encrypts keyj using the public key of node nj and sends the cipher text to nj. nj decrypts the cipher text using its private key to obtain keyj. S also announces two hash functions, H1 and HMAC key , to all nodes in PSD. H1 is unkeyed while HMAC key is a keyed hash function that will be used for message authentication purposes later on. Besides symmetric key distribution, S also needs to set up its HLA keys.

Packet Transmission Phase

After implementation the net phase, S enter the packet broadcast stage. S broadcast packet to PSD according to the following steps. Before sending out a packet Pi, anywhere i is a sequence number that uniquely identifies Pi, S computes and generates the HLA signatures of ri for node nj, as follows the node has received, and it relays to the next hop on the route. The last hop, i.e., node nK, only forwards Pi to the destination D. As proved in Theorem 4 in Section 4.3, the special structure of the one-way chained encryption construction in (4) dictates that an upstream node on the route cannot get a copy of the HLA signature intended for a downstream node, and thus the construction is resilient to the collusion model defined in Section 3.2. Note that here we consider the verification of the integrity of Pi as an orthogonal problem to that of verifying the tag tji. If the verification of Pi fails, node n1 should also stop forwarding the packet and should mark it accordingly in its proof-of-reception database.

Audit Phase

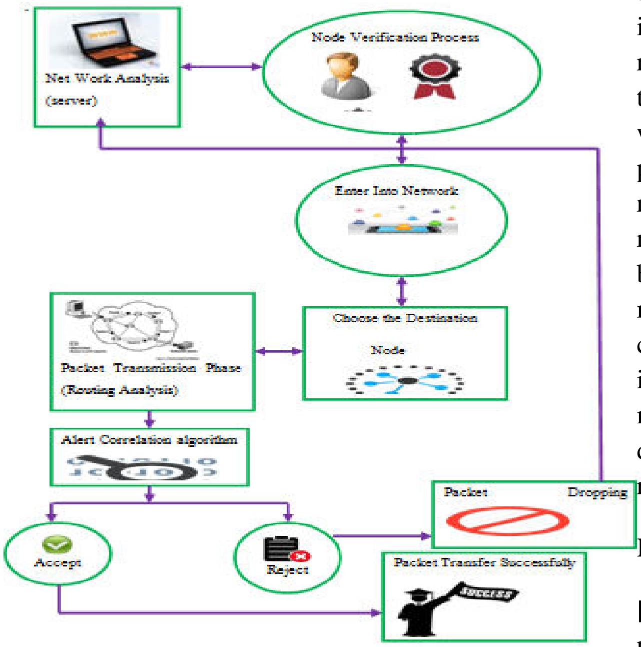
This stage is trigger as the free assessor Ad receives an ADR letter starting S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1; . . . ; nK, S's HLA public key information, the sequence numbers of the most recent M packets sent by S, and the sequence numbers of the subset of these M packets that were received by D. Recall that we assume the information sent by S and D is truthful, because detecting attacks is in their interest. Ad conducts the auditing process as follows. Ad submits a random challenge where the elements cji's are randomly chosen from Zp. Without loss of generality, let the sequence number of the packets recorded in the current proof-of-reception database be P1; . . . ; PM, with PM being the most recent packet sent by S. the above mechanism only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This mechanism cannot prevent a node from overly stating its packet loss by claiming that it did not receive a packet that it actually received.

Detection Phase

The civic assessor Ad enters the discovery phase after in receipt of and audit the respond to its confront from all nodes on PSD. The main tasks of Ad in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present.

Given the packet-reception bitmap at each node, b1; . . . ; ~b K, Ad first checks the consistency of the bitmaps for any possible overstatement of packet losses. Clearly, if there is no overstatement of packet loss, then the set of packets received at node j þ 1 should be a subset of the packets received at node j. since a usual lump forever honestly information its small package welcome, the small package-welcome bitmap of a hateful node that overstates its packet loss must contradict with the bitmap of a normal downstream node. Note that there is always at least one normal downstream node, i.e., the destination D. So Ad only needs to sequentially scan ~bj's and the report from D to identify nodes that are overstating their packet losses

ARCHITECTURE DIAGRAM


Net Work Analysis (server)
Node Verification Process
Enter Into Network
Choose the Destination Node
Packet Transmission Phase (Routing Analysis)
Alert Correlation algorithm
Packet Dropping
Accept
Reject
Packet Transfer Successfully
success

CONCLUSION

In this opinion we comprise attentive on spot nasty essentials booster in WSNs, in persnickety as one or auxiliary trial can be revealed and knowledge flanked by compromise sensors exploits the loss in correlation brought in by them. We have proposed a novel methodology to detect malicious data injections, based on the measurements cross-scale relationship. In adding, we have provide an come up to to typify hateful collude nodes, by partition the antenna nodes base on the association between their measurements. This approach considers the effects of events, hence it is able to detect groups of sensors that elicit or mask events. lastly, we provide a work of fiction capacity-based analysis method to tell apart fault-induce anomaly from hateful anomaly. We have tested the whole procedure by simulating sophisticated malicious injections on both a synthetic and a real dataset and we conclude that the detection gives highly reliable results. high-quality consequences have been achieve for the description and analysis stage, even although there is a considerable add to of complexity compared to detection. These are due to error propagation effects as well as to the complexity of the problem itself. In the prospect, we aim for a methodical recognition of the the majority intimidating hateful data injection, connected to the use rather than to the attacker's strategy. This would enable to study the effect of mobile sensors on performance, which is not trivial to test. furthermore, an analytical presentation assessment would eliminate the need for real malicious data which is currently difficult to retrieve. Finally, we plan to improve the diagnosis step by discriminating single faults and non-colluding malicious data injections. A possible approach is to characterize more properties of single faults, for instance through fault statistics or through a fault model. The latter could also model the temporal domain, which has been abstracted from since it is not reliable for detecting malicious data.

REFERENCES

[1] M. Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," J. Med. Syst., vol. 36, no. 1, pp. 93–101, 2010.

[2] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 51–58, Feb. 2010.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Future Generation Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad Hoc Netw., vol. 1, no. 2/3, pp. 293–315, 2003.

[5] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, pp. 53–57, 2004.

[6] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme

for wireless sensor networks." ACMTrans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.

[7] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks: A survey," ACM Comput. Surv., vol. 48, no. 2, pp. 24:1–24:33, Oct. 2015.

[8] L. M. A. Bettencourt, A. A. Hagberg, and L. B. Larkey, "Separating the wheat from the Chaff: Practical anomaly detection schemes in ecological applications of distributed sensor networks," in Proc. 3rd IEEE Int. Conf. Distrib. Comput. Sensor Syst., 2007, pp. 223–239.

[9] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. Bezdek, "Distributed anomaly detection in wireless sensor networks," in Proc. 10th IEEE Singapore Int. Conf. Commun. Syst., Oct. 2006, pp. 1–5.

[10] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Quarter sphere based distributed anomaly detection in wireless sensor networks," in Proc. IEEE Int. Conf. Commun., 2007, pp. 3864–3869.