Volume No:3, Issue No:8 (January-2018) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Protected and capable information broadcast for Cluster-based Wireless Sensor Networks

M.Suresh
Department of Computer Science, Sphoorthy Engineering College, Nadergul, Saroor Nagar, R.R.Dist, T S - 501510, India.

Mr.B.Venkanna
Department of Computer Science, Sphoorthy Engineering College, Nadergul, Saroor Nagar, R.R.Dist, T S - 501510, India.

J.Deepthi
Department of Computer Science, Sphoorthy Engineering College, Nadergul, Saroor Nagar, R.R.Dist, T S - 501510, India.

Abstract:

Secure data transmission is a critical issue for wireless sensor networks (WSNs).Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain.

SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

INTRODUCTION:

AWIRELESS sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN **[1].** Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings **[2]**. Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs.

WIRLESS SENSOR NETWORK:

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Cite this article as: M.Suresh, Mr.B.Venkanna & J.Deepthi, "Protected and capable information broadcast for Cluster-based Wireless Sensor Networks", International Journal of Research in Advanced Computer Science Engineering, Volume 3, Issue 8, 2018, Page 1-6.

Volume No:3, Issue No:8 (January-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

OBJECTIVES:

- To detect the wormhole attack and reduce the false aggregated data in wireless sensor network
- To improve the performance of iteration filtering algorithm against wormhole attack

Existing System:

- In recent years, there has been an increasing amount of literature on IF algorithms for trust and reputation systems. The performance of IF algorithms in the presence of different types of faults and simple false data injection attacks has been studied where it was applied to compressive sensing data in WSNs.
- In the past literature it was found that these algorithms exhibit better robustness compared to the simple averaging techniques; however, the past research did not take into account more sophisticated collusion attack scenarios. If the attackers have a high level of knowledge about the aggregation algorithm and its parameters, they can conduct sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes.

DISADVANTAGES OF EXISTING SYSTEM:

- Although the existing IF algorithms consider simple cheating behaviour by adversaries, none of them take into account sophisticated malicious scenarios such as collusion attacks.
- Although the existing IF algorithms consider simple cheating behaviour by adversaries, none of them take into account sophisticated malicious scenarios such as collusion attacks.

Proposed System:

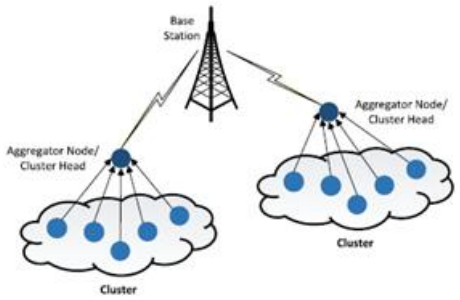
- A new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection. In such an attack scenario, colluders attempt to skew the aggregate value by forcing such IF algorithms to converge to skewed values provided by one of the attackers.
- In this paper, we propose a solution for vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors.
- Identification of a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms.
- A novel method for estimation of sensors' errors which is effective in a wide range of sensor faults and not susceptible to the described attack.
- Design of an efficient and robust aggregation method inspired by the MLE, which utilises an estimate of the noise parameters obtained using contribution above.
- Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions.

Volume No:3, Issue No:8 (January-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

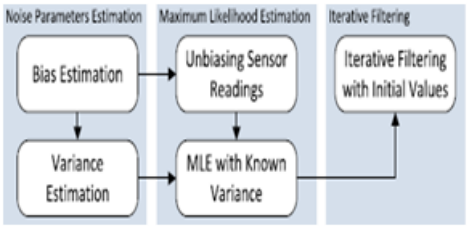
ADVANTAGES OF PROPOSED SYSTEM:

We provide a thorough empirical evaluation of effectiveness and efficiency of our proposed aggregation method. The results show that our method provides both higher accuracy and better collusion resistance than the existing methods.To the best of our knowledge, no existing work addresses on false data injection for a number of simple attack scenarios, in the case of a collusion attack by compromised nodes in a manner which employs high level knowledge about data aggregation algorithm used.

SYSTEM ARCHITECTURE:



BLOCK DIAGRAM:



IMPLEMENTATION:

Use is the period of the assignment when the speculative blueprint is changed out into a working structure. Thusly it can be believed to be the most essential stage in achieving a productive new structure and in giving the customer, assurance that the new system will work and be suitable. The utilization compose incorporates mindful orchestrating, examination of the present structure and it's confinements on execution, arranging of procedures to finish changeover and appraisal of changeover strategies.

Module Description:

- Setting up Network Model
- Robust Data Aggregation
- Enhanced Iterative Filtering
- Accuracy with a Collusion Attack

MODULES DESCSRIPTION:

Setting up Network Model:

Our first module is setting up the network model. We consider a large-scale, homogeneous sensor network consisting of resource-constrained sensor nodes. The sensor nodes are divided into disjoint clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically collected and aggregated by the aggregator. We assume that each data aggregator has enough computational power to run an IF algorithm for data aggregation.

Robust Data Aggregation:

In order to improve the performance of IF algorithms against the aforementioned attack scenario, we provide a robust initial estimation of the trustworthiness of sensor nodes to be used in the first iteration of the IF algorithm. Most of the traditional statistical estimation methods for variance involve use of the sample mean. For this reason, proposing a robust variance estimation method in the case of skewed sample mean is an essential part of our methodology.

We assume that the stochastic components of sensor errors are independent random variables with a Gaussian distribution; however, our experiments show that our method works quite well for other types of errors without any modification. Moreover, if error distribution of sensors is either known or estimated, our algorithms can be adapted to other distributions to achieve an optimal performance. Based on such an estimation of the bias and variance of each sensor, the bias estimate is subtracted from sensors readings and in the next phase of the proposed framework, we provide an initial estimate of the reputation vector calculated using the MLE.

Volume No:3, Issue No:8 (January-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Enhanced Iterative Filtering:

According to the proposed attack scenario, the attacker exploits the vulnerability of the IF algorithms which originates from a wrong assumption about the initial trustworthiness of sensors. Our contribution to address this shortcoming is to employ the results of the proposed robust data aggregation technique as the initial reputation for these algorithms. Moreover, the initial weights for all sensor nodes can be computed based on the distance of sensors readings to such an initial reputation. Our experimental results illustrate that this idea not only consolidates the IF algorithms against the proposed attack scenario, but using this initial reputation improves the efficiency of the IF algorithms by reducing the number of iterations needed to approach a stationary point within the prescribed tolerance.

Accuracy with a Collusion Attack:

In order to illustrate the robustness of the proposed data aggregation method in the presence of sophisticated attacks, we synthetically generate several data sets by injecting the proposed collusion attacks. Therefore, we assume that the adversary employs c ($c < n$) compromised sensor nodes to launch the sophisticated attack scenario proposed. The attacker uses the first compromised nodes to generate outlier readings in order to skew the simple average of all sensor readings. The adversary then falsifies the last sensor readings by injecting the values very close to such skewed average. This collusion attack scenario makes the IF algorithm to converge to a wrong stationary point. In order to investigate the accuracy of the IF algorithms with this collusion attack scenario, we synthetically generate several data sets with different values for sensors variances as well as various number of compromised nodes. The results of this experiment validate that our sophisticated attack scenario is caused by the discovered vulnerability in the IF algorithms which sharply diminishes the contributions of benign sensor nodes when one of the sensor nodes reports a value very close to the simple average.

LITERATURE SURVEY:

1) Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults:

Wireless sensor networks (WSNs) enable the collection of physical measurements over a large geographic area. It is often the case that we are interested in computing and tracking the spatial-average of the sensor measurements over a region of the WSN. Unfortunately, the standard average operation is not robust because it is highly susceptible to sensor faults and heterogeneous measurement noise. In this paper, we propose a computational efficient method to compute a weighted average (which we will call robust average) of sensor measurements, which appropriately takes sensor faults and sensor noise into consideration. We assume that the sensors in the WSN use random projections to compress the data and send the compressed data to the data fusion centre. Computational efficiency of our method is achieved by having the data fusion centre work directly with the compressed data streams. The key advantage of our proposed method is that the data fusion centre only needs to perform decompression once to compute the robust average, thus greatly reducing the computational requirements. We apply our proposed method to the data collected from two WSN deployments to demonstrate its efficiency and accuracy.

2) Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures:

As the trust issue in wireless **[4]** sensor networks is emerging as one important factor in security schemes, it is necessary to analyze how to resist attacks with a trust scheme. In this we categorize various types of attacks and countermeasures related to trust schemes in WSNs.

Volume No:3, Issue No:8 (January-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Furthermore, we provide the development of trust mechanisms, give a short summarization of classical trust methodologies and emphasize the challenges of trust scheme in WSNs. An extensive literature survey **[3]** is presented by summarizing state-of-the-art trust mechanisms in two categories: secure routing and secure data. Based on the analysis of attacks and the existing research, an open field and future direction with trust mechanisms in WSNs is provided.

3) Measuring quality, reputation and trust in online communities:

In the Internet era the information overload and the challenge to detect quality content has raised the issue of how to rank both resources and users in online communities. In this paper we develop a general ranking method that can simultaneously evaluate users' reputation and objects' quality in an iterative procedure, and that exploits the trust relationships and social acquaintances of users as an additional source of information. We test our method on two real online communities, the EconoPhysics forum and the Last.fm music catalogue, and determine how different variants of the algorithm influence the resultant ranking. We show the benefits of considering trust relationships, and define the form of the algorithm better apt to common situations.

4) Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks:

Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN.

As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. In this paper we demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce. To address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.

5) Spatial correlation-based collaborative medium access control in wireless sensor networks:

Wireless Sensor Networks (WSN) are mainly characterized by dense deployment of sensor nodes which collectively transmit information about sensed events to the sink. Due to the spatial correlation between sensor nodes subject to observed events, it may not be necessary for every sensor node to transmit its data. This paper shows how the spatial correlation can be exploited on the Medium Access Control (MAC) layer. To the best of our knowledge, this is the first effort which exploits spatial correlation in WSN on the MAC layer. A theoretical framework is developed for transmission regulation of sensor nodes under a distortion constraint. It is shown that a sensor node can act as a representative node for several other sensor nodes observing the correlated data. Based on the theoretical framework, a distributed, spatial Correlation-based Collaborative Medium Access Control (CC-MAC) protocol is then designed which has two components:

Volume No:3, Issue No:8 (January-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Event MAC (E-MAC) and Network MAC (N-MAC). E-MAC filters out the correlation in sensor records while N-MAC prioritizes the transmission of route-thru packets. Simulation results show that CC-MAC achieves high performance in terms energy, packet drop rate, and latency.

CONCLUSION:

We introduced a novel collusion attack scenario against a number of existing IF algorithms. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging. In future work, we will investigate whether our approach can protect against compromised aggregators. We also plan to implement our approach in a deployed sensor network.

REFERENCES:

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput. Intell.Springer-Verlag, 2010, vol. 278.

[2] Y. Wang, G. Waterbury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol. 8, no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Comput. Commun. vol. 30, no. 14-15, pp.2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670,2002.