ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

CAFS: Cluster based Authentication scheme for Filtering False data in wireless Sensor network

Uma Narayanan[1], Arun Soman[2]

Department of Information Technology, Rajagiri School of Engineering and Technology, Rajagiri valley, Cochin, India[1]

Assistant Professor, Department of Information Technology, Rajagiri School of Engineering and Technology, Rajagiri valley, Cochin, India [2]

Abstract: Wireless sensor is an emerging technology that has resulted in variety of application. Wireless sensor networks offer unique benefits and versatility for those locations and applications where human interaction is less feasible, examples of which may be to monitor volcanoes, movements inside enemy territory or temperature and humidity deep inside a machinery, to count a few. Wireless sensor networks can provide low cost solution to verity of real-world problems. Due to its tiny size it is easy to be compromised. So when a node is compromised it is easy to inject false data in to the network. It is burden to sink to verify the false data. In this paper, we propose a Cluster based authentication scheme for filtering injected false data in wireless sensor network. Based on elliptical curve cryptography, Diffe - Hellman key management technique and using Cooperative authentication scheme with CNR based MAC code technique; the proposed scheme can save energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink, which thus largely reduces the burden of the sink. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high filtering probability and energy saving.

Keywords: Include at least 4 keywords or phrases

I. INTRODUCTION

Wireless sensor networks have extensively been the focus of research in the recent years. Such networks are composed of several hundred to several thousand of sensors disseminated in a geographical area. Sensors are very simple, battery powered electronic devices equipped with a tiny processor, few kilobytes of storage memory, a radio transceiver and sometimes a mobilizer depending upon the application.

Wireless sensor networks offer unique benefits and versatility for those locations and applications where human interaction is less feasible, examples of which may be to monitor volcanoes, movements inside enemy territory or temperature and humidity deep inside a machinery, to count a few. With no prerequisites of fixed infrastructure or base stations, they can be created and used anytime, anywhere. Such networks could be inherently fault-resilient, for they do not operate under the limitations of a fixed topology. The addition and deletion of nodes is easy and might sometimes only require dropping a few hundred through a vehicle. These types of networks have many advantages where setting up wired line networks is not possible. Such advantages have attracted immediate attention in its use among military, police, and rescue agencies, and especially under disorganized or hostile environments, including isolated scenes of natural disaster and armed conflict.

WSN is an emerging technology that has resulted in a variety of applications. Many applications such as health care, medical diagnostics, disaster management, military surveillance and emergency response have been deploying such networks as their main monitoring framework. Basically, a wireless sensor network consists of a number of tiny sensor nodes connected together through wireless links. Some more powerful nodes may operate as control nodes called base stations. Often, the sensing nodes are referred to as “motes” while base stations are sometimes called “sinks”. Each sensor node can sense data such as temperature, humidity, pressure from its surroundings, conduct simple computations on the collected data and send it to other neighboring nodes through the communication links. Control nodes may further process the data and probably transfer it to a database server via a wired connection.

Wireless sensor networks are expected to interact with the physical world at an unprecedented level to enable various new applications. However, a large-scale sensor network may be deployed in a potentially adverse or even hostile environment and potential threats can range from

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

accidental node failures to intentional tampering. Due to their relatively small sizes and unattended operations, sensor nodes have a high risk of being captured and compromised. False sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in a battery powered network. Although several recent research efforts [1]–[3] have proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions can only prevent false reports injection by outside attackers. They are rendered ineffective when any single node is compromised (Fig. 1). To combat false reports injected by compromised nodes, one must have means to detect such false reports.

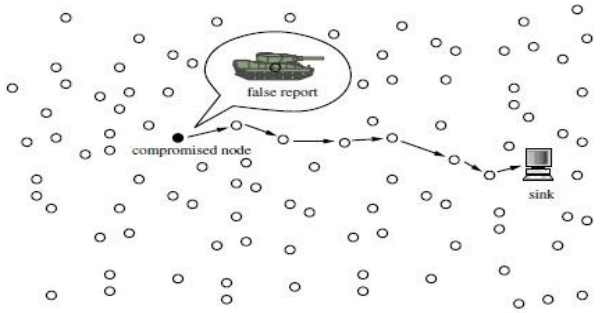

Figure 1: False report of compromised node

This paper deals with preventing false data that is been injected in wireless sensor network with rekey management and clustering. In wireless sensor network different types of attacks on transit is considered in Section II. Section III is about the recent works in WSN. IV is about the improved version of existing system in which the life time of the network is increased considerably .The security of the wireless sensor network is another challenging research area. In which we have improved the security of sensor network by applying different security features. In section V is simulation of the proposed system CAFS. Then paper ends with the conclusion of the CAFS.

II. ATTACKS ON TRANSIT IN WIRELESS SENSOR NETWORK

It is a type of attack which affects the data that is being sent. Since sensed data is the inevitable part of sensor network, its compromise cannot be entertained. So we can consider this attack as one of the hot research area in the field of network security. In this paper we are going to suggest a method to avoid the one of the attacks in WSN on transit. Attack on transit can be broadly classified as follows.

A. Interruption

Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption and insertion of malicious code.

B. Interception

Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it.

C. Modification

Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with false data.

D. False data injection

Sensor nodes are not tamper resistant and can be easily compromised by an adversary. In this attack an adversary injects false data and compromises the trust worthiness of the information communicated. False sensing reports can be injected through compromised nodes. To prevent the injection of false data in WSN can be prevented by using CAFS Method. CAFS method can be effectively applicable to military purpose also where confidentiality and integrity is main focus. The proposed system can be easily implemented in wireless sensor network.

III. RELATED WORK

Recently, some research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature in [3], [4], [5], [6],[7]. In [3], Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. As the report being forwarded, each node along the way verifies the correctness of the MACs at earliest point. If the injected false data escapes the en-routing filtering and is delivered to the sink, the sink will further verify the correctness of each MAC carried in each report and reject false ones.

In SEF, to verify the MACs, each node gets a random subset of the keys of size k from the global key pool of size N and uses them to producing the MACs. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. By simulation, SEF can prevent the injecting false data attack with 80-90 percent probability within 10 hops. However, since n should not be large enough as described above, the filtering probability at each en-routing node $p = k(T - Nc)/N$ is relatively low. Besides, SEF does not consider the N possibility of en-routing nodes' compromise, which is also crucial to the false data filtering.

In [4], Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

along the path, one is the lower association node, and the other is the upper association node. An en-routing node will forward received report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses t þ 1 individual MACs by XORing them to one. By analyses, only if less than t nodes are compromised, the sink can detect the injected false data. However, the security of the scheme is mainly contingent upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed. In addition, as pointed in [2], Zhu et al.'s scheme, similar as SEF, also adopts the symmetric keys from a key pool, which allows the compromised nodes to abuse these keys to generate false reports. Location-Based Resilient Secrecy (LBRS) is proposed by Yang et al. [5], which adopts location key binding mechanism to reduce the damage caused by node compromise, and further mitigate the false data generation in wireless sensor networks.

In [6], Ren et al. propose more efficient location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability. Because LEDS is a symmetric key based solution, to achieve en-routing filtering, it requires location-aware key management, where each node should share at least one authentication key with one node in its upstream/downstream report-*auth cell*.

In [7], Zhang et al. provide a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms. To achieve en-routing filtering, additional 20 bytes authentication overheads are required. Bit-compressed authentication technology can achieve bandwidth-efficient, which has been adopted in some research works [8], [9].

In [8], Canetti et al. use one-bit authentication to achieve multicast security. The basic idea in multicast is very similar to the BECAN scheme, where a source knows a set of keys R ={K1 , . . . , K*l*}, each recipient *u* knows a subset R*u* & R. When the source sends a message M, it authenticates M with each of the keys, using a MAC. That is, a message M is accompanied with (MAC(K1, M1), . . . , MAC(K*l* , M*l*)) Each recipient u verifies all the MACs which were created using the keys in its subset Ru . If any of these MACs is incorrect, the message M will be rejected. To achieve the bandwidth efficiency, each MAC is compressed as single bit. The security of the scheme is based on the assumption that the source is not compromised. However, once the source is compromised, the scheme obviously does not work. Therefore, it cannot be applied to filter false data injected by compromised nodes in wireless sensor networks.

In [9], Benenson et al. also use 1-bit MACs to decide whether a query is legitimate in wireless sensor networks. However, similar as that in [8], once the source is compromised, the 1-bit MACs also does not work. Different from the above works, the proposed BECAN scheme adopts CNR based filtering mechanism together with multireports technology. Because of non inter-active key establishment, BECAN does not require a complicated security association [4], [6]. In addition, BECAN considers the scenario that each node could be compromised with probability *p*, i.e., some en-routing nodes could be compromised. To avoid putting all eggs in one basket, BECAN distributes the en-routing authentication to all sensor nodes along the routing path. To save the bandwidth, it also adopts the bit-compressed authentication technique. Therefore, it is compromise-tolerant and suitable for filtering false data in wireless sensor networks.

IV. PROPOSED SYSTEM

This to be deleted Proposed system is a cluster based authentication system and also use rekey management scheme which improve the life time and security of sensor network when compared with the existing system. The proposed system use elliptical curve cryptography, Diffie-Hellman key management, AES algorithm and Rekey Management. These help to improve the performance and the life time of the sensor network with more security and less overhead.

The senor network now gaining more importance in every filed which lead to importance of security measures. Our CAFS play major role in the field of security. So CAFS can be implemented easily and effective in Sensor network and shows high result.

A. Elliptical Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman.

ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

B. Diffie Hellman Key Exchange

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

C. Rekey Management

The keys used in WSNs have to be refreshed periodically. Rekeying is also performed on demand or upon the high vulnerability of revealing any key polynomials. Rekeying is the most important phase in the dynamic key management and enhances the resilience against a node capture and a collusion attack. In our scheme rekeying is performed in localized manner. In secure group communications, users of a group share a common group key. A key server sends the group key to authorized new users as well as performs group rekeying for group users whenever the key changes. Each cluster has a proper number of KGNs (Key Generation Node) which make it difficult that an attacker can reveal the network keys by capturing some KGNs. In upper layer, rekeying is performed using the secret key between BS and sensor node i. The secret key is preloaded in each sensor node with unique ID and authenticates the node to the BS. The BS generates one t-degree bivariate polynomial key and distributes it by means of session key shared by all CHs. This makes the communication between CHs efficient.

D. Description of Cluster base Authentication

The first phase of project deals with creation of sensor nodes and its initiation. Number of sensor nodes are created and it is divided in to cluster according to the distance using LEACH-selective cluster Algorithm. The LEACH- SC makes use of the distance and identifies the cluster heads, which has shown considerable improvement in the network life time in wireless sensor network. One of the scare resources of sensor network is its battery, once battery is out sensor nodes are of no use. By make use of clustering we can improve overall performance of wireless sensor network. After the selection of Cluster heads we identify Source for sending data to the sink. After selection of source node then key pair establishment is done. This is done using diffie-hellmen key management. This secret is used to generate CNR based MAC code. The message and time stamp is send to the cluster head by AES Encryption. Then Message is decrypted and cluster head generate Mac code and verify the Mac code .If MAC code matches with the existing one then it is mark as accepted else it is marked as rejected. This process continue till it reaches the destination i.e., sink.

The Sink only check whether the all the cluster head has marked as accepted, if all has marked as accepted then message will be accepted else the message is dropped. The burden of the sink is reduced considerably because it only has to check for the marked one other job are already done by the cluster heads .The Injected False data is Thus filtered by Node in the path itself, if somehow it reaches the sink, it will be filtered by sink node. In existing system the sink has the burden of verifying the data and the do necessary mechanism to verify the authentication of message. Another advantage of this proposed system it uses the Rekey management. The flow chart of the proposed system is given below in fig 2.

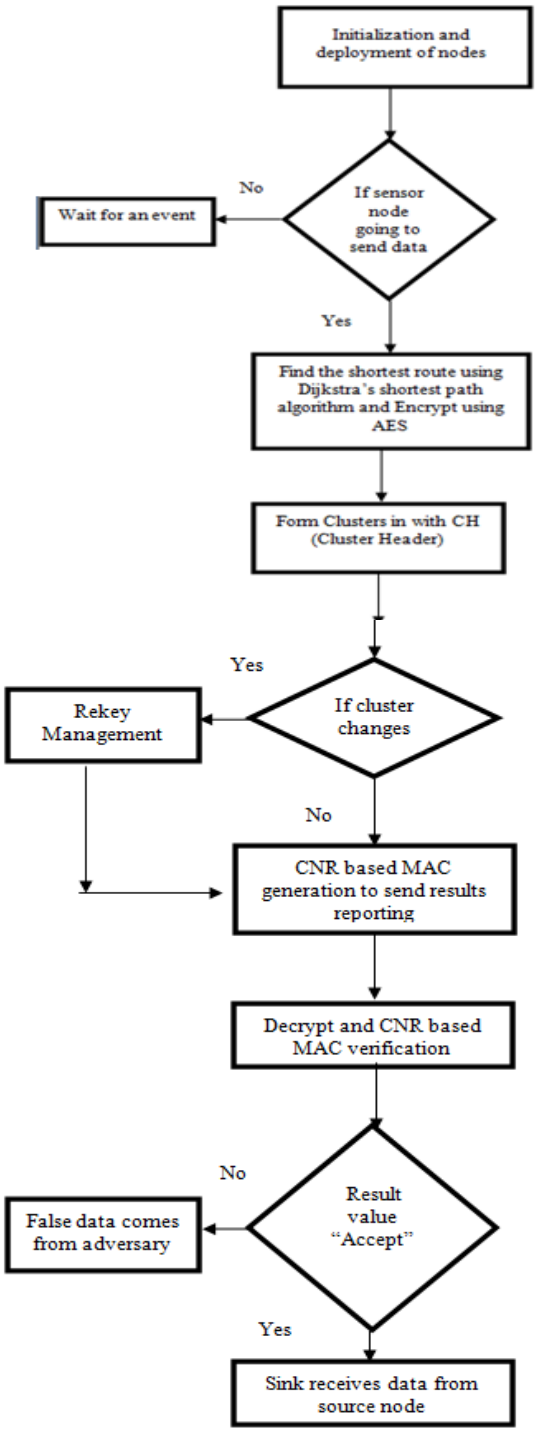

Fig 2: Flow chart of CAFS

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

V. SIMULATION

Simulation is done using Java simulator. The main constrain is the power, battery of the senor node are the scare resource .In case of nodes once the battery dies out sensor nodes are of no use , so main objective is to improve the life time of sensor nodes and effectively prevent injected false data that is been transmitted in sensor network. Our proposed CAFS show considerable improvement in the field of power consumption and also prevent the false data, thus providing security for wireless sensor network. Simulation result proves the above scenario, fig 3 and fig 4 proves the improvement when compared with existing system.

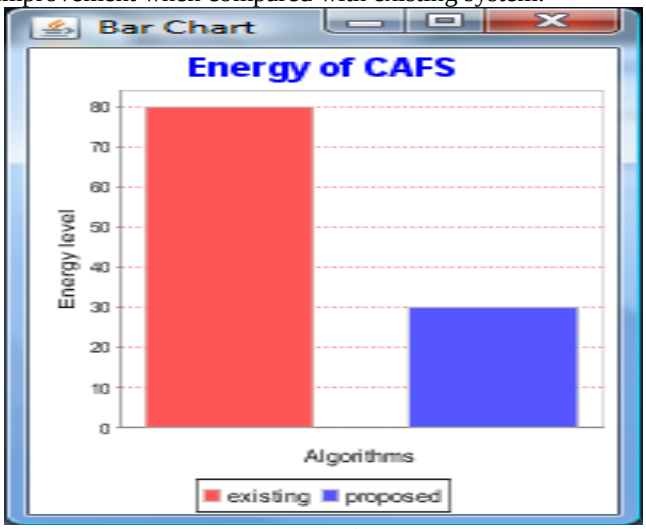

Fig 3: Energy usage of sensor nodes.

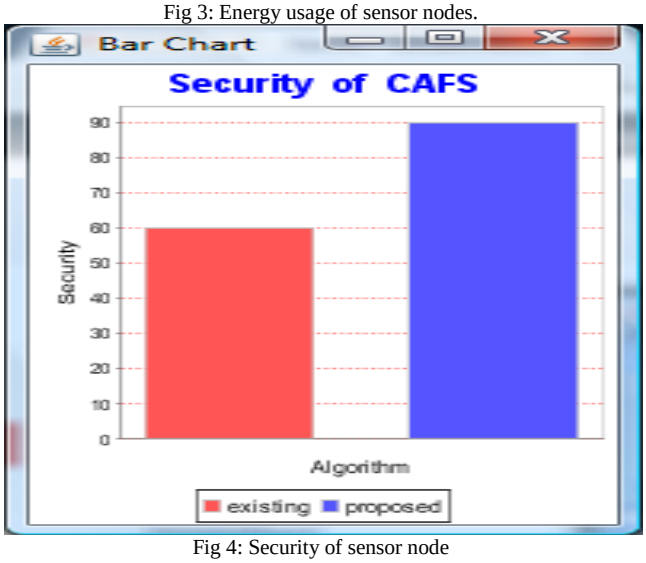

Fig 4: Security of sensor node

VI. CONCLUSION

We can conclude that the total energy consumption and security mobile wireless sensor network are increasing with the growth of network size. When we adapt the Rekey management, the total energy consumption and pocket delay can be effectively reduced. Sensing data can be reliably transmitted, and network is connectivity at all moments in the state. CAFS can be applied to the scenarios with mobile sensor nodes effectively and shows significant improvement in filtering false data in wireless sensor network, reduce the burden of Sink.

REFERENCES

[1] Rongxing Lu, Xiaodong Lin, Member, Haojin Zhu, Xiaohui Liang and Xuemin (Sherman) Shen, BECAN: "A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", IEEE Parallel and Distributed System, 2012.

[2] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[3] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc.IEEE INFOCOM '04, Mar. 2004.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[5] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05),pp. 2005.

[6] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM '06, Apr. 2006.

[7] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 247- 260, Feb. 2006.

[8] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B.Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions," Proc. IEEE INFOCOM '99, pp. 708-716, Mar. 1999.

[9] Z. Benenson, C. Freiling, E. Hammerschmidt, S. Lucks, and L.Pimenidis, "Authenticated Query Flooding in Sensor Networks,"Security and Privacy in Dynamic Environments, Springer, pp. 38-49,July 2006.

[10] X. Lin, R. Lu, P. Ho, X. Shen, and Z. Cao, "TUA: A NovelCompromise-Resilient Authentication Architecture for WirelessMesh Networks," IEEE Trans. Wireless Comm., vol. 7, no. 4,pp. 1389-1399, Apr. 2008.

[11] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks,"Proc. IEEE INFOCOM '08, Apr. 2008