Detecting False Data in Wireless Sensor Network using BECAN Seceme

[1]S.*SAJITHABANU*, [2]*M.DURAIRAJ*

[1]Assistant Professor, Department of MCA Mohamed Sadak Engineering College,Kilakarai,Tamilnadu,India.
[2]Assistant Professor, Department of Computer Science Bharathidasan University,Trichy, Tamilnadu,India.

Abstract
Wireless sensor networks (WSNs) as an emerging technology faces numerous challenges. Sensor nodes are usually resource constrained. Sensor nodes are also vulnerable to physical attacks or node compromises. As the projected applications for wireless sensor networks range from smart applications such as traffic monitoring to critical military applications such as measuring levels of gas concentration in battle fields, security in sensor networks becomes a prime concern. In sensitive applications, it becomes imperative to continuously monitor the transient state of the system rather than steady state observations and take requisite preventive and corrective actions. The network is prone to attack by adversaries who intend to disrupt the functioning of the system by compromising the sensor nodes and injecting false data into the network. So it is important to shield the sensor network from false data injection attacks. We use a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data based on Bloom Filter.

Keywords:
Wireless Sensor Networks, Bandwidth, Injecting false data attack, Bloom Filter.

1. Introduction

Wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components [1].

Wireless sensor network is a collection of nodes organized into a cooperative network [2]. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni- directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators.

The advancements in micro electronics and wireless communications have led to the creation of the wireless sensor network (WSN) technology. This technology has many applications, including various environmental monitoring. A primitive objective of WSNs is to answer queries by gathering sensory data from the deployed sensors; the process of collecting Sensory data is often called "in-network processing" or "aggregation". Since sensor nodes in WSN technology are usually tiny micro-electronic devices which have limited resources (low processor speed, small memory size, low computation and communication power), it becomes very challenging to design mechanisms to support data queries.

1.1 Wireless Sensor Networks

Wireless sensor networks (WSNs) have recently emerged as a 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 [2]. 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 from its surroundings (e.g. temperature, humidity, pressure), 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. Figure 1 shows a typical architecture for a WSN. The sensing nodes "motes" are represented by black spheres and are responsible for observing the surrounding environment whereas the cube represents a control node "sink" which serves as the base station.

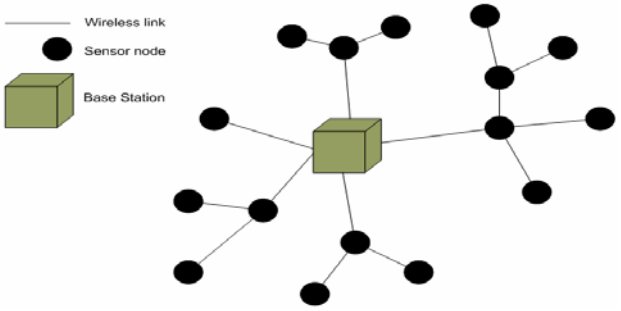

Figure 1. Typical WSN Architecture

Manuscript received March 5, 2013
Manuscript revised March 20, 2013

2. SYSTEM MODELS AND ASSUMPTIONS

2.1 Sensor Network Model

We consider a sensor network composed of a large number of small sensor nodes. We further assume that the sensor nodes are deployed in high density, so that a stimulus (e.g., a tank) can be detected by multiple sensors. Each of the detecting sensors reports its sensed signal density and one of them is elected as the center-of-stimulus (CoS) node. The CoS collects and summarizes all the received detection results, and produces a synthesized report on behalf of the group. The report is then forwarded toward the sink, potentially traversing a large number of hops (e.g., tens or more). The sink is a data collection center with sufficient computation and storage capabilities, and it may also implement advanced security solutions to protect itself.

Due to cost constraints we assume that each sensor node is not equipped with tamper-resistant hardware. However, dense deployment enables cross-verification of a reported event among multiple sensors even in the presence of one or more compromised nodes. SEF design harnesses the advantage of large-scale. Rather than relying on a small number of powerful and expensive sensors, SEF utilizes large numbers of small sensors for reliable sensing and reporting.

2.2 Threat Model

We assume that the attacker may know the basic approaches of the deployed security mechanisms, and may be able to either compromise a node through the radio communication channel, or even physically capture a node to obtain the security information installed in the node. However, we assume that attackers cannot subvert the data collection unit, i.e., the sink, because the protection at the sink is powerful enough to defeat such subversion efforts. Once compromised, a node can be used to inject false reports into the sensor network. Node and message authentication mechanisms [4]–[6] prevent naive impersonation of a sensor node. However, they cannot block false injection of sensing reports by compromised nodes.

Besides false data injection, a compromised sensor node can launch various other attacks. It can stall the generation of reports for real events, block legitimate reports from passing through it (which we call false negative attacks), or record and replay old reports, etc. As the first effort in tackling the threats from compromised components, this paper focuses on the detection of false event reports, which we call false positives attacks, injected by compromised nodes. We plan to address other attacks in subsequent efforts.

3. Existing System

Most of these filtering mechanisms use the symmetric key technique, once a node is compromised, it is hard to identify the node. Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and Sybil attacks. In addition, wireless sensor networks may also suffer from injecting false data attack. For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper-level error decision, as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report wrong wildfire location information to the sink, and then expensive resources will be wasted by sending rescue workers to a non-existing or wrong wildfire location. Therefore, it is crucial to filter the false data as accurately as possible in wireless sensor networks. At the same time, if all false data are flooding into the sink simultaneously, then not only huge energy will be wasted in the en-route nodes, but also heavy verification burdens will undoubtedly fall on the sink. As a result, the whole network could be paralyzed quickly. Therefore, filtering false data should also be executed as early as possible to mitigate the energy waste. Since most of these filtering mechanisms use the symmetric key technique, once a node is compromised, it is hard to identify the node. In other words, the compromised node can abuse its keys to generate false reports, and the reliability of the filtering mechanisms will be degraded.[1]

4. Proposed system

We propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks using Bloom Filter. Compared with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability. And also prevent the gang injecting false data attack from mobile compromised sensor nodes using AODV routing protocol.

4.1 Architecture model

We consider a typical wireless sensor network which consists of a sink and a large number of sensor nodes $N = \{N_0, N_1, \ldots\}$ randomly deployed at a certain interest region (CIR) with the area S. The sink is a trustable and powerful data collection device, which has sufficient computation and storage capabilities and is responsible for

initializing the sensor nodes and collecting the data sensed by these nodes

The communication is bidirectional,i.e., two sensor nodes within their wireless transmission range (R) may communicate with each other. If a sensor node is close to the sink, it can directly contact the sink. If a sensor node is far from the transmission range of the sink, it should resort to other nodes to establish a route and then communicate with the sink.

Sensor Nodes Initialization Algorithm

1: Procedure SENSORNODESINITIALIZATION
Input: params and un-initialized N={N0,N1,N2, .. .}
Output: initialized N={N0,N1,N2, . . }
2: for each sensor node Ni £ N do
3: preload Ni with pair wise key, params and energy
4: choose a random prime number x_i £ Z_q as the private key, compute the public key Yi= x_iG, and install (Y_i; x_i) in Ni
5: end for
6: return initialized N ={N_0, N1, N2, . . .N_n}
7: end procedure

4.2 En-routing

The attacker cannot generate correct MACs of other T Nc distinct categories. To produce seemingly legitimate reports has to forge T−Nc key indices of distinct partitions and T−Nc MACs.We first compute the probability that a forwarding node has one of the T − Nc keys, thus being able to detecting an incorrect MAC and drop the report. We use the Bloom filter here. In this module first form the routing using MAC. Next check whether the routing is secure or not. If the routing is secure then forwarding the data to one node to other.

4.3 Security analysis

We analyze the security of the BECAN authentication scheme with respect to our main design goal,i.e., the effectiveness of filtering the injected false data. We use pair wise shared security scheme for BECAN.Key generation and establishment done in this module.RSA algorithm used for generate pair wise key.

4.3.1 Simulation –Based Bloom Filtering Evaluation

In the simulation, the bloom filtering probability can be tested as

FPR =Number of false data filtered by en- route nodes

Total number of false data

In what follows, we provide the simulation results for FPR.

4.3.2 Simulation Settings

We study FPR of the BECAN scheme using a Network Simulator. In the simulations, 1,000 sensor nodes with a transmission range R are randomly deployed in a CIR of region 200 × 200 m2 interest region. We consider each sensor node could be compromised with the probability ρ. In Table 1, we list the simulation parameters. Then, we test the networks when the number of en-routing nodes in the interest areas is varied from 5 to 15 in increment of 1. For each case, 10,000 networks are randomly generated, and the average of bloom filtering probabilities over all of these randomly sampled networks are reported.

TABLE 1 Parameter Settings

Parameter	Value
Simulation area	200m ×200m
Number of Sensor nodes	1000
Transmission range R	20m,25m
Compromised Probability	2%
# Neighboring nodes k	4,6
#Routing nodes l	2,…,10

4.4 Sink Verification

The sink receives the report (m T MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m,T,MAC) will be immediately discarded. Otherwise, the sink looks up all private keys kis of Ni,0<=i<=k , and invokes the Algorithm . If the returned value of algorithm is accept the sink accepts the report m otherwise the sink rejects the report.

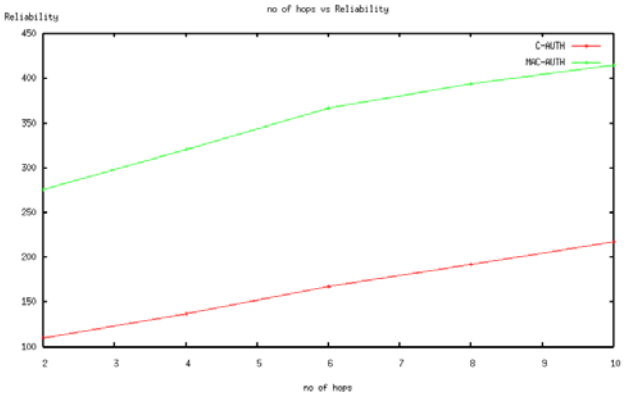

Fig.2. Reliability of the BECAN scheme

4.5 Performance Evaluation

In this section, we analyze the computational and communication overheads of our basic scheme. Energy saving is always crucial for the lifetime of wireless sensor networks. In this module, the performance of the proposed BECAN scheme is evaluated in terms of energy efficiency. In this scheme first check the security, then check the throughput and delay of the packet radio. It produces the graph analysis report. And also evaluate Energy Consumption in Noninteractive key pair establishment and Evaluate Energy Consumption in Transmission. The BECAN scheme could be applied to other fast and distributed authentication scenarios.

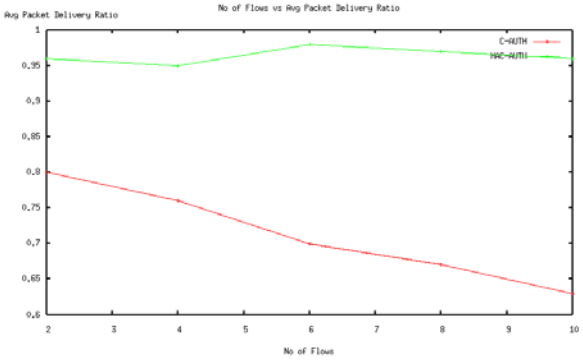

Fig.3. Performance Evaluation for Packet delivery radio

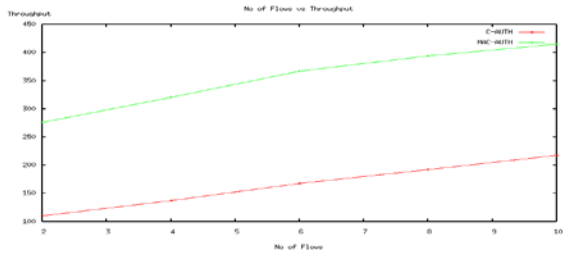

Fig.4. Performance Evaluation for Throughput

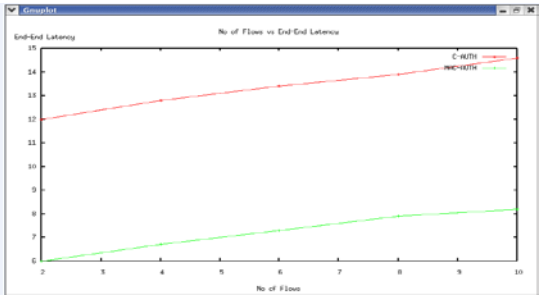

Fig.5. Performance Evaluation for End to End Latency

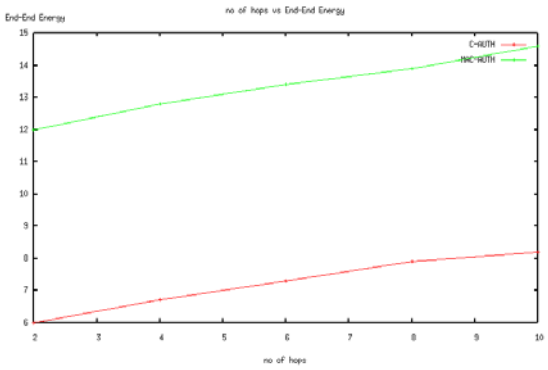

Fig.6. Performance Evaluation for End to End Energy

5. Related Work

Sensor network security has been studied in recent year in a number of proposals. Recently, some research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature in [8], [9], [10], [11],[12]. In [8], 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 possibility of en-routing nodes' compromise, which is also crucial to the false data filtering. In [9], 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 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 + 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 [7], 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. [10], 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 [11],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 [12], 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.

SEF key assignment bears similarities with [15], which use probabilistic key sharing to establish trust between neighboring nodes. Chan et al. [15] further trades off the unlikelihood of large scale attacks for higher strength against smaller ones.

To achieve enroute filtering, based on bloom filter additional 20 bytes authentication overheads are required. Bit-compressed authentication technology can achieve bandwidth-efficient, which has been adopted in some research works [13], [14]. In [13], 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,...,Kl} , each recipient u knows a subset Ru 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,M),…, MAC(Kl,M)› 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 [14], Benenson et al. also use 1-bit MACs to decide whether a query is legitimate in wireless sensor networks. However, similar as that in [13],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 multi reports technology. Because of non interactive key establishment, BECAN does not require a complicated security association [9], [11]. In addition, BECAN considers the scenario that each node could be compromised with probability _, 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.

6. Conclusion

In this paper, we proposed a novel BECAN scheme for filtering the injected false data based on Bloom filter, and conduct thorough theoretical analysis on the related topics. The BECAN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi-reports. We evaluated the performance for packet delivery ratio, throughput and end to end latency of the proposed system The BECAN scheme could be applied to other fast and distributed authentication scenarios. The extensive simulation results sufficiently demonstrate that the proposal presents remarkable performances on communication cost, energy consumption balance, and security. And also prevented the gang injecting false data attack from mobile compromised sensor nodes using AODV routing protocol.

References

[1] Rongxing Lu, Xiaodong Lin, 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 Transactions on Parallel and Distributed Systems, vol. 23, no. 1, January 2012.

[2] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System rchitecture Directions for Networked Sensors, SPLOS, November 2000.

[3] Nirupama Bulusu, Sanjay Jha, "Wireless Sensor Networks, A Systems Perspective",ISBN:1-58053-867-3, 2005.

[4] R. Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An Analysis of a Large Scale Habit Monitoring Application," Proc. Second ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '04), 2004.

[5] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), 2002.

[6] R. Lu, X. Lin, C. Zhang, H. Zhu, P. Ho, and X. Shen, "AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '08), May 2008.

[7] 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
[8] 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.
[9] 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.
[10] 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. 34-45, 2005.
[11] 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.
[12] 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.
[13] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, “Multicast Security: A Taxonomy and Some EfficientConstructions,” Proc. IEEE INFOCOM ’99, pp. 708-716, Mar. 1999.
[14] 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.
[15] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” in IEEE Symposium on Security and Privacy,2003.

Dr. M. Durairaj has received Ph.D. degree in Computer Science from the Bharathidasan University, Thiruchirappalli, India on the year 2011. He is currently working as an Assistant Professor in Department of Computer Science & Engineering, Bharathidasan University. He has been associated with the Indian Council of Agricultural Research for 12 years and involved in various research projects. His fields of expertise include Data Mining, Soft computing, Artificial Neural Networks and Rough Sets. He Has 16 Publications to his credit in National and International Journals.

S.SAJITHABANU is doing II year M.Tech[IT] in Bharathidasan University , Trichy. She received B.Sc degree in Computer Science at Thassim Beevi Abdul Kader College for Women ,Kilakarai from Madurai Kamaraj University and M.Sc degree in Computer Science from Alagappa University, Karaikudi,India and M.Phil degree in Computer Science from Madurai Kamaraj University,India. Currently She is working as a Assistant Professor in Mohamed Sadak Engineering College ,Kilakarai. She has published Cloud Security paper in International Journal.