International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 3, June 2014, PP 145-151
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data using timer in Wireless Sensor Networks

Laxmi Shabadi[1], Snehal .T[2], Sanjana .H[3], Kalavati .G[4], Anita .K[5]

Department of Computer Science and Engineering
BLDEA's Dr.P.G.Halkatti College of Engineering and Technology,
(Affilated to Visvesvaraya Technological University),Bijapur, India.
laxmishabadi07@gmail.com

Abstract: *Injecting false data attack is a well-known serious threat to wireless sensor network, for which an adversary reports bogus information to sink causing error decision at upper level and energy waste in en-route nodes. In this paper, we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data. This uses fixed timer to filter the packets in prior. The proposed BECAN scheme uses Random graph characteristics of sensor node deployment, Co-operative Neighbour Router(CNR) to save energy by early detecting and filtering the most of injected false data with less time and difficulty at en-route nodes. In addition, only a very small amount of injected false data needs to be checked by the sink, thereby reducing the burden on sink. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed BECAN scheme in terms of high filtering probability and energy saving*

Keywords: *BECAN, Cooperative Neighbor Router, Random graph characteristics, Timestamp.*

1. INTRODUCTION

Due to the fast booming of micro electro mechanical systems, wireless sensor networking has been subject to extensive research efforts in recent years. It has been well recognized as a ubiquitous and general approach for some emerging applications, such as environmental and habitat monitoring, surveillance and tracking for military. A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. A sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components. Therefore, when a sensor node generates a report after being triggered by a special event, e.g., a surrounding temperature change, it will send the report to a data collection unit (also known as sink) through an established routing path.

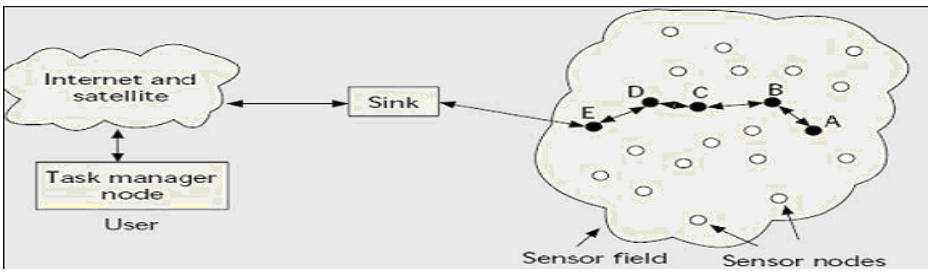

Figure 1.1 *Basic Architecture of the sensor network*

Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, 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 a wrong wildfire location information to the sink, 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.

In this paper, we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. Compared

with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability. The main contributions of this paper are

threefold.

- First, we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication;
- Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient; and
- Third, we develop a custom Java simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

2. RELATED WORK

In [1], 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. 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. SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering.

In [2], 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.

3. IMPLEMENTATION AND METHODOLOGY

3.1 Modules

✓ **Sensor Node Initialization**

In this module, the key server generates unique public and private keys for each sensor node and sink. These keys will be shared to the sensor nodes when they start.

✓ **CNR Based MAC Generation**

This technique is used by the sensor nodes for generating authentication message. This technique uses Elliptic curve cryptography and DES algorithm.

✓ **CNR Based MAC Verification**

In this phase, the sink verifies the authentication message sent by sensor node using ECC algorithm.

✓ **Sink Verification**

In this module, the sink verifies each message sent by sensor nodes weather it is valid or invalid.

3.2 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

Let p be a large prime and E(IFp)represent an elliptic curve defined over IFp. Let G €E(IFp)be a base point of prime order q. Then, each sensor nodeNi € N can preload a TinyECC based public-private key pair (Yi, xi), where the private key xi is randomly chosen from Z*q and the public key Yi =xi, G. Non- interactive key pair establishment. For any two sensor nodes vi, vj€ G = (V,ε) no matter what eij€{0,1} is, sensor nodes vi with the key pair (Yi, xi) and vj with the key pair (Yj,xj) can establish a secure Elliptic Curve Diffie-Hellman (ECDH) key pair without direct contacting, where

kij=xiYj=xixjG=xjxiG=xjYi=kji. (1)

vi and vj can secretly share a key. At the same time, the established keys are independent.

In other words, if a sensor node vi is compromised, then the key kij shared between vi and vj will be disclosed. However, the key kjj` shared between vj and another sensor node vj` is not affected.

3.3 Design Rationale

To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor router(CNR)-based filtering mechanism. As shown in Fig

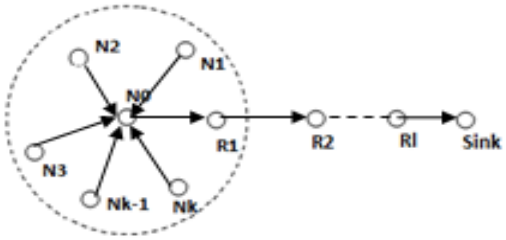

Figure 3. *Cooperative CNR-Based authentication mechanism*

CNR-based mechanism, when a source node N0 is ready to send a report m to the sink via an established routing path RN0 : [R1 -> R2 ->. . Rl-> Sink], it first resorts to its k neighboring nodes NN0 : {N1,N2, . . .,Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 U NN0 to the sink via routing RN0.

4. RESULTS AND DISCUSSION

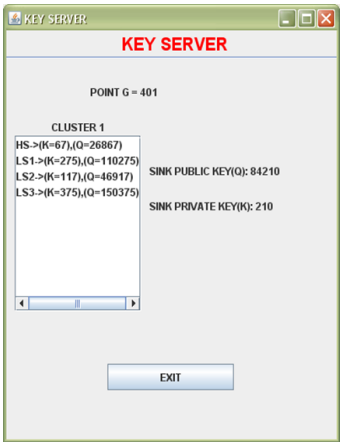

Figure 4.1 *Initial part of project*

Interpretation :-The below window shows the cluster head. Where we can see that the cluster head owns its public and private keys as well as knows the public keys of all the sensors which are made to communicate with cluster head

Figure 4.2. *Cluster head window*

Interpretation: -The below snap shows the window of each sensor that is deployed. Where we can see its own private and public keys and even public key of the sink.

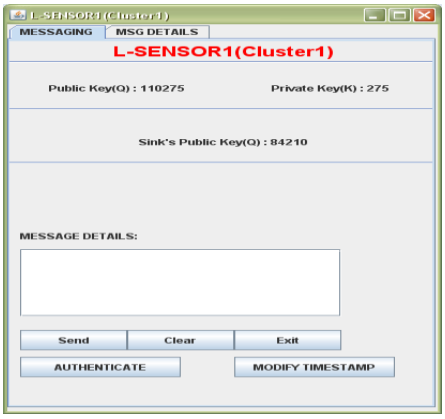

Figure 4.3. *Single sensor window*

Interpretation:-Below window shows the sink, with authentication status, sensor name, sensor route, message, delay (which is also the timer specification)and status of the message which indicates the message is authenticated or no.

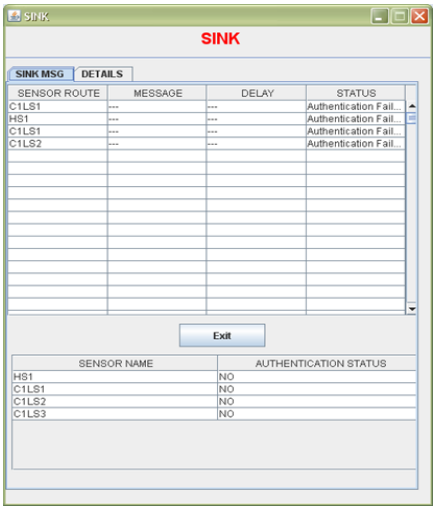

Figure 4.4. *Message sent when there is no authentication*

Interpretation: - The window shown below clearly explains that only a single node is been authenticated i.e. sensor 1 which you can see in the authentication status. Similarly the remaining nodes are not authenticated and the message is not received by the sink. And we can also observe that the node which is authenticated sends the message within the time threshold. That's the reason we see the status as normal.

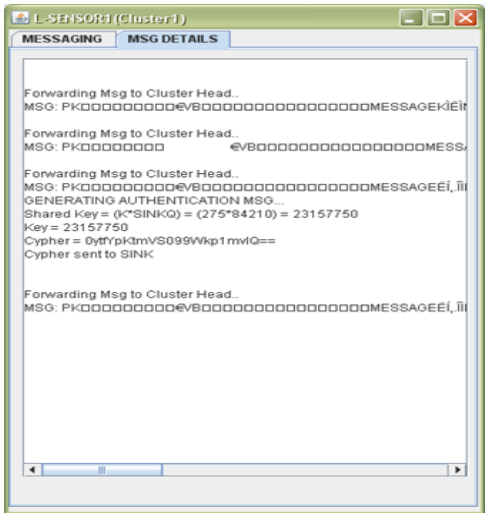

Figure 4.5. *Message at the sensor1*

Interpretation: - The window below shows the details of the message at the sensor node which is sending the message.

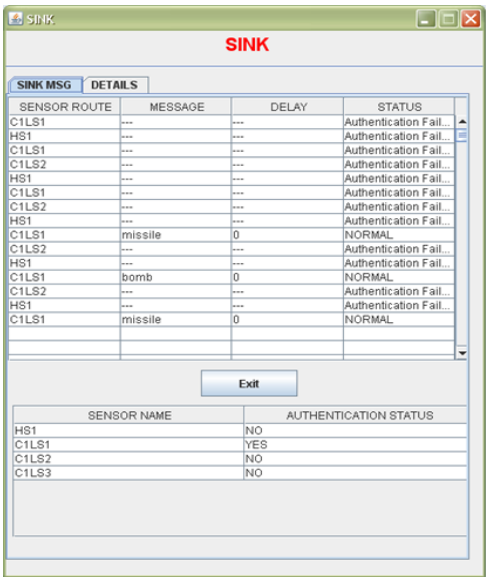

Figure 4.6 : *Window shows when node is authenticated.*

Interpretation: - The window below shows how the sensor node sends the message randomly. And we can also see that the authenticate button should be clicked to make each node authenticate with the sink.

5. CONCLUSION

In this paper, we have proposed a novel BECAN scheme for filtering the injected false data. This scheme achieves not only high en-routing filtering probability but also high reliability with multi-reports and timestamp. Due to this the BECAN scheme could be applied to the other fast and distributed network where authentication purpose is also distributed, e.g., authentication function in wireless mesh network. BECAN does not require complex security fixation because it uses non-interactive key establishment. In our future work, we will investigate how to prevent or reduce the gang injecting false data on mobile compromised sensor nodes.

REFERENCES

[1] 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.

[2] 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. IEEESymp.Security and Privacy, 2004.

[3] 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.

[4] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security In Wireless Sensor Netwroks," Proc. IEEE INFCOM 06, Apr. 2006.

[5] 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.274-260, Feb. 2006.

[6] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "A Dos-Resilient En-Route Filtering Scheme for sensor Networks," Proc. Tenth ACM Int'l Symp.Mobile Ad Hoc Networking and Computing (MobiHoc'09),pp. 343-344, 2009.

[7] J. Chen, Q. Yu, Y. Zhang, H.-H. Chen, and Y. Sun, "Feedback Based Clock Synchronization in Wireless Sensor Networks: A Control Theoretic Approach," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2963-2973, June 2010.

[8] S. He, J. Chen, Y. Sun, D.K.Y. Yau, and N.K. Yip, "On Optimal Information Capture by Energy-Constrained Mobile Sensors," IEEE Trans. Vehicular Technology,vol. 59, no.5, pp. 2472-2484, June 2010.

[9] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. Seventh Int'l Conf Information Processing in Sensor Networks (IPSN'08),pp. 245-256, Apr. 2008.

[10] J. Dong, Q. Chen, and Z. Niu, "Random Graph Theory BasedConnectivity Analysis in Wireless Sensor Networkswith Rayleigh Fading Channels," Proc. Asia-Pacific Conf. Comm.(APCC '07),pp. 123-126, Oct. 2007.

AUTHOR'S BIOGRAPHY

Prof. Laxmi Shabadi, working as assistant professor in V.P Dr. P.G Halakatti college of engineering and technology, Bijapur. She completed B.E and M.tech in computer science and engineering from Visvesvaraya Technological University, Karnataka, INDIA, in 2011. Her research interests are image processing and computer networks.

Snehal T has received B.E (Computer Science & Engineering) degree from V.P Dr. P.G Halakatti college of engineering and technology, Visvesvaraya Technological University, Karnataka, INDIA, with distinction in 2014. Her areas of interest are Image Processing, Signal Processing and Computer Networks.

Sanjana H has received B.E (Computer Science & Engineering) degree from V.P Dr. P.G Halakatti college of engineering and technology, Visvesvaraya Technological University, Karnataka, INDIA, with distinction in 2014. Her areas of interest are Image Processing, Signal Processing and ComputerNetworks.

Kalavati G has received B.E (Computer Science & Engineering) degree from V.P Dr. P.G Halakatti college of engineering and technology, Visvesvaraya Technological University, Karnataka, INDIA, with first class in 2014. Her areas of interest are Image Processing, Signal Processing and ComputerNetworks.

Anita K has received B.E (Computer Science & Engineering) degree from V.P Dr. P.G Halakatti college of engineering and technology, Visvesvaraya Technological University, Karnataka, INDIA, with first class in 2014. Her areas of interest are Image Processing, Signal Processing and ComputerNetworks.