IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Filtering False Data Injection Using Becan Scheme in Wireless Sensor Networks

V.Chitra[1], L.Hameetha Begum[2], M.Ramya[3], R.Udhaya[4]

[1, 2, 3, 4]**Assistant Professor, Department of Information Technology, P.S.R.Rengasamy College of Engineering for Women**

Abstract

False Data injection is a serious threat in wireless sensor networks. Injecting false data attack is the one in which opponent reports fake information to sink that will create a error at top and energy waste in en-route nodes . To detect and filter the false data injectionin the early stage, this paper proposes BECAN Scheme. It can save energy by early detecting and filtering the majority of injected false data using CNR authentication technique and random graph generation.

KEY WORDS—*Wireless sensor network, injecting false data attack, random graph, cooperative bit-compressed authentication.*

1. INTRODUCTION

Due to the fast booming of microelectro 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 applications[1][2][5].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. Each 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 [17].Wireless sensor networks are usually deployed at unattended or hostil environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and sybil attacks [12],[18]. In addition, wireless sensor networks may also suffer from injecting false data [10]. 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. To tackle this challenging issue, some false data filtering mechanisms have been developed [7], [8], [9], [10], [11], [12], [13]. 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. 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 thershold.The rest of the paper is organized as follows. The related works are described in Section 2. The proposed scheme is well explained in Section 3. The simulation model is demonstrated

in Section 4. In final, conclusion and future work is detailed in Section5.

2 RELATED WORKS

2.1TinyECC-Based Noninteractive Keypair Establishment

TinyECC is a configurable library for Elliptic Curve Cryptography (ECC), which allows flexible integration of ECC-based public key cryptography in sensor network applications. A substantially experimental evaluation using representative sensor platforms, such as MICAz [21] and Imote2 [22], is performed, and the results show that the ready-to-use TinyECC is suitable for wireless sensor networks to provide convenient authentications and pair key establishments [19]. Let p be a large prime and E(IFp) represent an elliptic curve defined over IFp. Let G ЄE(IFp) be a base point of prime order q. Then, each sensor node Ni ЄN can preload a TinyECC based public-private key pair (Yi=xi),where the private key xi is randomly chosen from Zz*q and the public key Yi =xiG.

Non interactive key pair establishment.

For any two sensor nodes vi, vj Є G=(V,ε), no matter what eij Є {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) keypair without direct contacting[23], where kij =xiYj =xixjG = xjxiG =xjYi = kji. (5)Because of the hardness of Elliptic Curve Discrete Logarithm (ECDL) problem, only 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. For unattended wireless sensor networks, the property of key independence is useful, since itcan limit the scope of key disclosure to the adversary A.

2.2 Message Authentication Code in Zz2^n

Message authentication code (MAC) provides assurance tothe recipient of the message which came from the expected sender and has n to been altered in transit [24]. Let h(.) be asecure cryptographic hash function [25]. A MAC in Zz2^n can be considered as a keyed hash, and defined as,

MAC(m,k,n)=h(m||k)mod2^n,

where m,k, n are a message, a key, and an adjustableparameter, respectively. When n =1,MAC(m,k,1) provides one-bit authentication, which can filter a false messagewith the probability 1/2 ; while n=α, MAC(m,k,α) can filter a false message with a higher probability 1-1/2^α.

The main problem of existing system is:

- Energy wasted in en-route nodes.
- Heavy verification burdens.
- Gang injecting false data attack.
- No Cooperative Authentication.
- Smaller key size.

3 PROPOSED SCHEME

A novel bandwidth-efficient co-operative authentication (BECAN) scheme for filtering injected false data. Based on the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique, the proposed BECAN 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.

3.1.BECAN Scheme

A novel bandwidth-efficient co-operative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. Then compared with the previously a reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability.

•) 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;

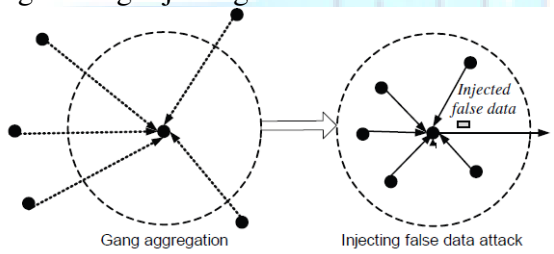
•) Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In

addition,the accompanied authentication information is bandwidth-efficient; and
•) Third, we develop a custom simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

3.2.Early detecting the injected false data by the en-route sensor nodes

The sink is a powerful data collection device. Nevertheless, if all authentication tasks are fulfilled at the sink, it is undoubted that the sink becomes a bottleneck. At the same time, if too many injected false data flood into the sink, the sink will surly suffer from the Denial of Service (DoS) attack. Therefore, it is critical to share the authentication tasks with the en-route sensor nodes such that the injected false data can be detected and discarded early. The earlier the injected false data are detected, the more energy can be saved in the whole network.

Fig 1.Gang injecting false data attack



3.3.Gang Injecting False Data attacker

We introduce a new stronger injecting false data attack, called gang injecting false data attack, in wireless sensor networks. This kind of attack is usually launched by a gang of compromised sensor nodes controlled and moved by an adversary A. As shown in Fig. 2, when a compromised source node is ready to send a false data, several compromised nodes will first move and aggregate at the source node, and then collude to inject the false data. Because of the mobility, the gang injecting false data attack is more challenging and hard to resist.

3.4.Reliability of the BECAN scheme

In addition to the high (en-routing) filtering probability, the BECAN scheme also has high reliability, i.e., even though some sensor nodes are compromised, the true event reports still can reach the sink with high probability. Let FNR be the false negative rate on the true reports and tested asIf FNR is small, the BECAN scheme is demonstrated high reliability.

$$\text{FNR} = \frac{\text{number of true data that cannot reach the sink}}{\text{total number of true data}}$$

4 SIMULATION RESULTS

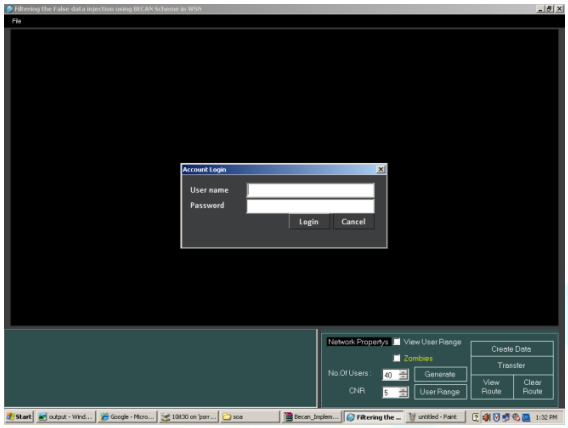
The language C# are used for our project. C# is an elegant and type-safe object-oriented language that enables developers to build a variety of secure and robust applications that run on the .NET Framework. Visual C# provides an advanced code editor, convenient user interface designers, integrated debugger, and many other tools to make it easier to develop applications based on the C# language and the .NET Framework. Output are genetrated by the parameter settings.

Tab.1(a) Default Parameter Setting

S.NO	PARAMETER'S	VALUE'S
1	Simulation Area	200m x 200m
2	No.of Nodes	40 to 100
3	No.of Zombies	1 to 3
4	No.of Sensor Nodes	1 or 2
5	Node Range	120 to 350
6	Neigbouring Nodes	N(upto No.of Nodes we fixed in output)
7	No.of Sender and Receiver	One to Many &Many to One(Our Choice)
8	En-route Nodes	5 to 15

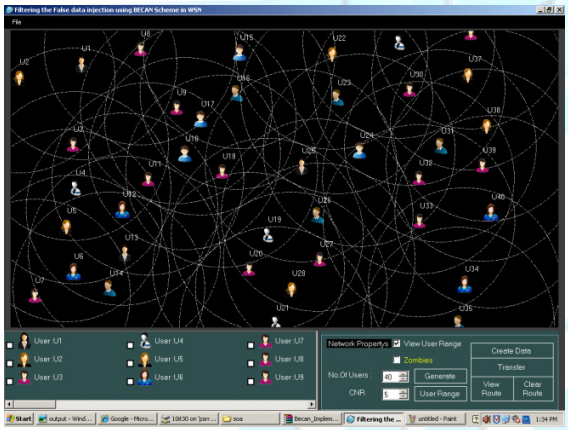
In our simulation,we first create an administration login to enter into the network.The username and password for administration login is created at first for entering into the process.

Fig.2 Login Page



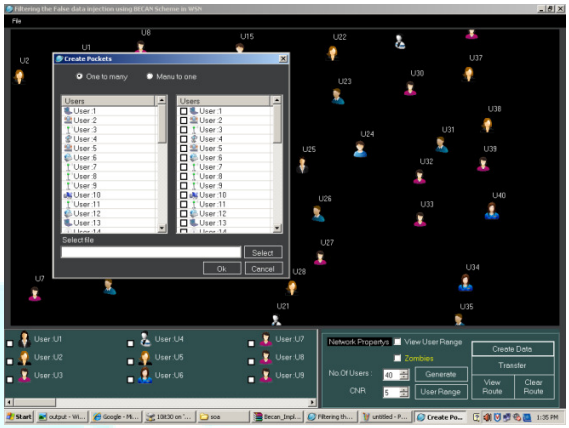
After enter into the process, automatically default no.of users can be generated.Then we fix a no.of users and their range by our choice.

Fig .3 Node Range



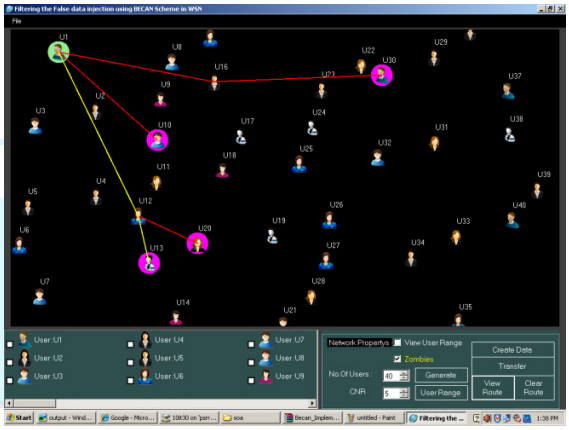
Then,we choose a no,of senders and receivers for transferring a selected packet.The packet may be either text,image,audio or video format.

Fig.4 Create Packet



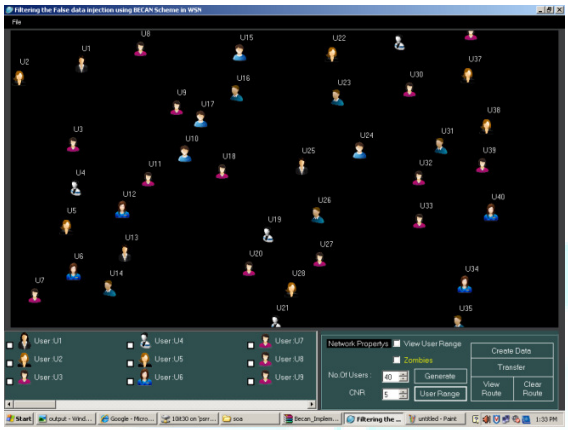
Between the sender and receiver a shortest path route will be created automatically to transfer the packet.The attacker is automatically generated to hack the packets between Sender and receiver and they will send the packet with false duplicate file to the receiver in the shortest path.The red line indicate the correct data transfer and the yellow line indicate false data transfe

Fig.5 Packet transfer with false duplicate file



Detective Node are generated automatically to detect and filter the false duplicate file in the packet and then send the correct packet to the receiver.

Fig.6 Receive Filtered Packet



For the above result,we make a change in the default parameter setting.

Tab.1(b)Output Parameter Setting

S.NO	PARAMETER'S	VALUE'S
1	Simulation Area	200m x 200m
2	No.of Nodes	40
3	No.of Zombies	2
4	No.of Sensor Nodes	1
5	Node Range	350
6	Neigbouring Nodes	5
7	No.of Sender and Receiver	One to Many (1 to 4)
8	En-route Nodes	3

REFERENCES

[1] 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.
[2] 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.
[3] K. Ren, W. Lou, and Y. Zhang, **"Multi-user Broadcast Authentication in Wireless Sensor Networks,"** Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.
[4] 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.
[5] Z. Zhu, Q. Tan, and P. Zhu, **"An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network,"** Proc.
10th Asia-Pacific Network Operations and Management Symp.(APNOMS '07), pp. 457-465, 2007.
[6] K. Akkaya and M. Younis, **"A Survey on Routing Protocols for Wireless Sensor Networks,"** Ad Hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.
[7] V.C. Giruka, M. Singhal, J. Royalty, and S. Varanasi**, "Security in Wireless Sensor Networks,"** Wireless Comm. and Mobile Computing, vol. 8, no. 1, pp. 1-24, Jan. 2008.
[8] 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.
[9] J. Dong, Q. Chen, and Z. Niu, **"Random Graph Theory Based Connectivity Analysis in Wireless Sensor Networks with Rayleigh**
Fading Channels," Proc. Asia-Pacific Conf. Comm. (APCC '07), pp. 123-126, Oct. 2007.
[10] **MICAz:Wireless Measurement System,** http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICAz_Data
sheet.pdf, 2010.
[11] **Imote2: High-Performance Wireless Sensor Network Node,**
http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/Imote2_Dat asheet.pdf, 2010.
[12] C. Boyd, W. Mao, and K.G. Paterson, **"Key Agreement Using Statically Keyed Authenticators,"** Proc. Second Int'l Conf. Applied Cryptography and Network Security C (ACNS '04), pp. 248-262, 2004.
[13] X. Li, N. Santoro, and I. Stojmenovic, **"Localized Distance- Sensitive Service Discovery in Wireless Sensor and Actor Networks,"** IEEE Trans. Computers, vol. 58, no. 9, pp. 1275-1288, Sept. 2009.
[14] X. Li, A. Nayak, D. Simplot-Ryl, and I. Stojmenovic, **"Sensor Placement in Sensor and Actuator Networks,"** Wireless Sensor and
Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication, Wiley, 2010.
[15] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, **"An Effective Key Management Scheme for Heterogeneous Sensor Networks,"** AdHoc Networks, vol. 5, pp. 24-34, Jan. 2007.
[16] 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.
[17] K. Ren, W. Lou, and Y. Zhang, **"Multi-User Broadcast Authenticationin Wireless Sensor Networks,"** Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.
[18] 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.

[19] 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.
[20]X.Lin,**"CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks,"** Proc. IEEE
GLOBECOM '09, Nov.-Dec. 2009.