AN EFFICIENT SAFE ROUTING FOR FORGED DATA IN WIRELESS SENSOR NETWORKS

N.Gopinath[1], Jyothsna Bandreddi[2]

[1]MCA Student, Dept of MCA, DRK College of Engineering and Technology, Hyderabad, Andhra Pradesh, India

[2]Assistant Professor, Dept of CSE, DRK College of Engineering and Technology, Hyderabad, Andhra Pradesh, India

ABSTRACT:

A promising technology which has faced a variety of challenges and resulted in a range of applications is a wireless sensor networks. To perform distributed sensing tasks, wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links. A serious threat to wireless sensor network is injecting false data attack, for which an adversary reports false information to sink causing error decision at upper level and energy waste in en-route nodes. In this paper, for filtering injected false data we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme. Based on the cooperative bit compressed authentication technique and random graph characteristics of sensor node deployment, 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. Moreover, a very small fraction of injected false data needs to be checked by the sink, so that it reduces the burden of the sink. The effectiveness of the proposed scheme in terms of high filtering probability and energy saving can be demonstrated by both imaginary and simulation results. **Keywords:** Forged Data, BECAN, Filtering Injecting, Wireless Sensor Networks, En-routed Nodes, Sink.

1. INTRODUCTION:

Wireless sensor network is a promising technology that has resulted in a variety of applications such as health care, medical diagnostics; military surveillance and emergency response have been deploying such networks as their main monitoring framework [1] [2]. A sensor network must not only report each significant result promptly, but also reject false reports injected by attackers [3]. To provide node and message authentication for sensor networks to prevent false report injection by an outside attacker have been projected in our latest research. In addition to cause fake alarms that can waste real-world response effort, false reports can exhaust the finite amount of energy resource in a battery powered network [4] [5]. However, when any single node is compromised then these proposed security mechanisms are rendered ineffective [6]. An adversary first compromises several sensor nodes and accesses all important materials stored in the nodes which is shown in fig 1, and then controls these nodes to inject false information and send the counterfeit data to the sink to cause upper-level error decision and energy wasted in en-route nodes for an injecting false data attack [7] [8]. The expensive resources will be wasted by sending rescue workers to a non-existing or wrong wildfire location by making an adversary a wildfire event or by reporting wrong wildfire location information to the sink.

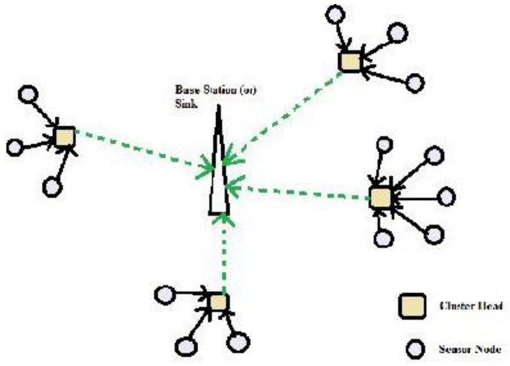

Fig 1: Cluster Based Wireless Sensor Network

Hence, it is crucial to filter the forged data as correctly as possible in wireless sensor networks and if all false data are flooding into the sink concurrently at the same time, then not only huge energy will be wasted in the en-route nodes, but also heavy authentication burdens will definitely fall on the sink and the whole network could be paralyzed quickly at the end [8] [9] [10]. Therefore, to mitigate the energy waste, filtering false data should also be executed as early as possible and some false data filtering mechanisms have been developed to tackle this challenging issue [11]. Since the symmetric key technique is the most used filtering mechanisms, it is hard to identify the node once a node is compromised [12] [13]. However, the compromised node can misuse its keys to generate false reports, and consistency of the filtering mechanisms will be corrupted. A novel bandwidth – efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks is proposed in this paper [14] [15].

2. SECURITY MODEL FOR FALSE DATA ATTACKS:

The BECAN scheme achieves not only high filtering probability but also high reliability compared with the previously reported mechanisms [16]. The three main contributions of this paper are: First, the probability of k-neighbors is estimated and provides the necessary condition for BECAN authentication and also the random graph characteristics of wireless sensor node deployment will be examined [17] [18]. Second, to filter the injected false data with cooperative bit-compressed authentication technique we propose a BECAN scheme. The injected false data can be early detected and filtered by the en-route sensor nodes with the proposed mechanism and the accompanied authentication information is bandwidth-efficient [19] [20]. Third, in terms of en-routing filtering probability and false negative rate on true reports, a custom Java simulator is developed to demonstrate the effectiveness of the proposed BECAN scheme. To degrade the network functionalities, since a wireless sensor network is unattended a malicious adversary may readily launch some security attacks. In addition, sensor nodes are not equipped with exclusive tamper-proof device and could be simply compromised in such vulnerable wireless sensor network due to the low-cost constraints. Therefore, we assume an adversary A can compromise a fraction of sensor nodes and obtain their stored keying materials in our security model. Then, to launch some injected false data attacks after being controlled and reprogrammed by the adversary A, these compromised sensor nodes can collude. By the compromised sensor nodes in wireless sensor network our work mainly focuses on filtering injected forged data attack and launched by other attacks, such as building false routing information, selectively reducing true data packet, and creating routing loops to devastate the energy of network are not addressed in this paper.

3. DETERMINATION OF GOAL:

For filtering the injected false data an efficient cooperative bandwidth-efficient authentication scheme is proposed in this paper. Specially, the two enviable objectives will be achieved. The sink is a influential data collection device. Nevertheless, the ink undoubtedly becomes a bottleneck if all authentication tasks are fulfilled at the sink. At the same times, the sink will surly suffer from the Denial of Service (DoS) attack if too many injected false data flood into the sink. Therefore, it is dangerous to share the validation tasks with the en-route sensor nodes such that the injected forged data can be detected and discarded early. The more energy can be saved in the whole network if the earlier the injected false data are detected. It is desirable to design a bandwidth efficient authentication scheme since the sensor nodes are low-cost and energy constraint. Newly, a statistical enrooting filtering mechanism called SEF is proposed and several research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature.

4. RESULTS:

A new stronger gang injecting false data attack was introduced in wireless sensor networks which were launched by a gang of negotiation sensor nodes controlled and moved by an adversary. Several compromised nodes will initially move and unite at the source node, and then get together to insert the false data when a concession source node is ready to send a false data. For the reason that the mobility of, the gang injecting false data attack is additional challenging and hard to resist. To tackle this attack, the multi-reports technology in BECAN scheme fits to the practical approach. Hence the BECAN scheme can attain high reliability. The BECAN system for each participating sensor node can make available its position information. If the existing position is not consistent with the preceding ones, the gang attack can be detected. However to prevent the gang injecting false data attack from mobile compromised sensor nodes is still worthy of the further investigation.

5. CONCLUSION:

In this paper, for filtering the injected false data we have proposed a new BECAN scheme. 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. The effectiveness of the proposed scheme in terms of high filtering probability and energy saving is demonstrated by both imaginary and simulation results. Due to the ease and efficiency, the BECAN scheme could be applied to other fast and distributed authentication scenarios. We will explore how to mitigate the gang injecting false data attack from mobile compromised sensor nodes in our future work.

REFERENCES:

[1] 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.

[2] 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.

[3] 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.

[4] X. Lin, R. Lu, and X. Shen, “MDPA: Multidimensional Privacy- Preserving Aggregation Scheme for Wireless Sensor Networks,” Wireless Comm. and Mobile Computing, vol. 10, pp. 843-856, 2010.

[5] X. Lin, “CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks,” Proc. IEEE GLOBECOM ’09, Nov.-Dec. 2009.

[6] 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.

[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] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “A dosresilient en-route filter- ing scheme for sensor networks,” in MobiHoc ’09: Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing. New York, NY, USA: ACM, 2009, pp. 343–344.

[15] 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 Transactions on Vehicular Technology, vol. 59, no. 6, pp. 2963–2973, June 2010.

[16] S. He, J. Chen, Y. Sun, D. K. Y. Yau, and N. K. Yip, "On optimal information capture by energyconstrained mobile sensors," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2472–2484, June 2010.
[17] 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.

[18] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," Wireless Communications and Mobile Computing, vol. 8, no. 1, pp. 1–24, January 2008.
[19] A. Liu and P. Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in IPSN 2008, April 2008, pp. 245– 256, sPOTS Track.
[20] J. Dong, Q. Chen, and Z. Niu, "Random graph theory based connectivity analysis in wireless sensor networks with rayleigh fading channels," in Asia-Pacific Conference APCC 2007, October 2007, pp. 123–126.

BIOGRAPHY:

N.GOPI NATH is pursuing his MCA from DRK College of Engineering and Technology, JNTU, Hyderabad, Andhra Pradesh, India. His main research interest includes PARALLEL AND DISTRIBUTED SYSTEMS.

Jyothsna Bandreddi has completed B.Tech, Koneru Lakshamaiah College of Engineering,Working as Assistant professor in department of Computer science and engineering of DRK College of engineering and technology. . Her main research interest includes Wireless Sensor Networks & Computer Networks.