Monitoring Cryptographic Strength of Wireless Sensor Networks using Knowledge-zero protocol

[1]V.Shanmukha Rao, [2]Aparna Allada, [3]Syed Ahmad Mohiddin

[1] Associate Professor,Dept of CSE, Andhra Loyola Institute of Engineering & Technology,Vijayawada, Krishna(Dist),Ap,India.

[2] Associate Professor, Department of CSE, Swarnandhra Engineering College, Narsapur,Ap,India.

[3] Associate Professor, Department of CSE Swarnandhra Engineering College, Narsapur,Ap,India.

ABSTRACT-The security mechanisms used for wired networks cannot be directly used in sensor networks as there is no user-controlling of each individual node, wireless environment, and more importantly, scarce energy resources. In this paper, we address some of the special security threats and attacks in Wireless Sensor Networks offer a powerful methodology to monitor environments, and have a lot of interesting applications, We propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself. The fingerprint is attached with every message a sensor node sends. The Zero knowledge protocol is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle attack and replay attack. The paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength.

Keywords: Wireless Sensor Networks, zero knowledge protocol cloning attack, man-in-the-middle attack.

1. INTRODUCTION

Wireless sensor networks consist of large numbers of sensors that act cooperatively to provide "usable chunks of predigested information rather than a confusing wash of number" [6]. A WSN provides refined information, i.e. it processes the raw data collected by individual sensors before presenting it to the user. This amounts to providing a service or a collection of services based on sensor capabilities and on the underlying communications infrastructure. Due to their vast array of applications, WSNs have been viewed from different perspectives and standpoints. Given the sensor capabilities, the next step is to have an operating system running on a sensor node. Such system has very restricted available resources but still has to provide required functionality and support for application development

When commodity hardware and operating systems are used, it is easy for an adversary to capture legitimate nodes, make clones by copying the cryptographic information, and deploying these clones back into the network. These clones may even be selectively reprogrammed to subvert the network. Individual sensor node contains a light weight processor, cheap hardware components, less memory. Because of these constraints, general-purpose security protocols are hardly appropriate. Public key cryptography is based on RSA approach. The energy consumption and computational latency makes RSA inappropriate for sensor network applications. Security algorithms that are designed specifically for sensor networks are found to be more suitable. The goal of this paper is to develop a security model for wireless sensor networks. We propose a method for identifying the compromised/cloned nodes and also verifying the authenticity of sender sensor nodes in wireless sensor network with the help of zero knowledge protocol.

1.1 Cryptographic Strength:

The cryptographic strength of ZKP is based on few hard to solve problems; the one which we have used in our scheme is based on the problem of factoring large numbers that are product of two or more large (hundreds of bits) primes. The values of

the public key also changes with every communication, making it more difficult for the attacker to guess it. The prover also generates a random number and the challenge also changes randomly. Thus, with a changed public key, challenge question from verifier and a new random number from the prover, it becomes extremely difficult for the attacker to break the security.

2. Related Work

2.1 Existing System

Existing Wireless sensor networks once sensor nodes have been deployed, there will be minimal manual intervention and monitoring. But, when nodes are deployed in a hostile environment and there is no manual monitoring

2.2 Proposed System

Nodes are divided into three categories; base station, cluster head and member nodes. Some arbitrary nodes are selected as cluster heads and generation of cluster heads is left to the clustering mechanism (not dealt in this work). Each cluster head knows about its member nodes, while every member node knows its cluster head. Base station stores information of all sensor nodes (including cluster heads). The base station maintains complete topological information about cluster heads and their respective members.

• Base station is powerful enough and cannot be compromised like other nodes of the network.

• There is no communication among the member nodes.

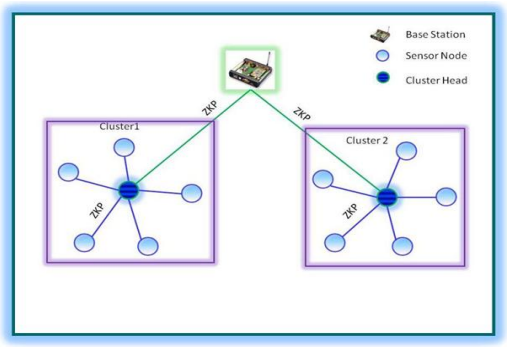

Fig: Zero knowledge protocol in the proposed model

Public key cryptography is based on RSA approach. The energy consumption and computational latency makes RSA inappropriate for sensor network applications. Security algorithms that are designed specifically for sensor networks are found to be more suitable. The goal of this paper is to develop a security model for wireless sensor networks. We propose a method for identifying the compromised/cloned nodes and also verifying the authenticity of sender sensor nodes in wireless sensor network with the help of zero knowledge protocol.

3. Modules in Implementation

3.1. Secure Zero-knowledge protocol

Zero-knowledge protocol allow identification, key exchange and other basic cryptographic operations to be implemented without revealing any secret information during the conversation and with smaller computational requirements in comparison to public key protocols. Thus ZKP seems to be very attractive for resource constrained devices. ZKP allows one party to prove its knowledge of a secret to another party without ever revealing the secret. ZKP is an interactive proof system which involves a prover, P and verifier, V. The role of the prover is to convince the verifier of some secret through a series of communications.

3. 2. Clone Attack

In clone attack, an adversary may capture a sensor node and copy the cryptographic information to another node known as cloned node. Then this cloned sensor node can be installed to capture the information of the network. The adversary can also inject false information, or manipulate the information passing through cloned nodes. Continuous physical monitoring of nodes is not possible to detect potential tampering and cloning. Thus reliable and fast schemes for detection are necessary to combat these attacks.

3.3. Man in the Middle Attack

The man-in-the-middle attack (MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection. The attacker will be able to intercept all messages exchanging between the two victims and inject new ones.

3.4. Replay Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by adversary who intercepts the data and retransmits it. This type of attack can easily overrule encryption.

4. System Description and Assumptions

We consider a network composed of N stationary, identical sensor nodes. Sensors are uniformly distributed over a disk Sink. Network topology of the reference scenario of unit radius
in the plane. The sink node collecting all information gathered by the sensors is located at the center of the disk. An example of network topology is shown in fig. 1, in the case of N = 400. We assume that all nodes have a common maximum radio range r and are equipped with omni directional antennas. Nodes can choose an arbitrary transmit power level for each data transmission, provided that their transmission range does not exceed r. Also, we consider network topologies such that for any sensor there exists at least one path connecting the sensor to the sink. The information sensed by a network node is organized into data units of fixed size that can be stored at the sensor in a buffer of infinite capacity; the buffer is modeled as a centralized FIFO queue. Sensors cannot simultaneously transmit and receive; the time is divided into time slots of unit duration and the transmission/reception of each data unit takes one time slot. The wireless channel is assumed to be error-free, although our model could be easily extended to represent a channel error process. Further assumptions on sensors behavior, traffic routing and channel access control are introduced below

5. Conclusions and Future Work

In this paper, we considered a sensor network where nodes send their data to a sink node by using multihop transmissions. To save energy, sensors alternate between two operational modes: sleep and active mode. While in sleep mode sensors consume lower power, their functional capabilities are also reduced. We developed an analytical model which enables us to investigate the trade-offs existing between energy saving and system performance, as the sensors dynamics in sleep/active mode vary. We were able to analytically derive several performance metrics, among which the distribution of the data delivery delay. By comparing analytical and simulation results we validated our model and showed the good accuracy of the proposed approach. To the best of our knowledge, this is the first analytical model that specifically represents the sensor dynamics in sleep/active mode, while taking into account channel contention and routing issues. The model could be easily modified to take into account some aspects that have not been addressed in this work and that can be interesting subject of future research. For instance, a model of the error process over the wireless channel can be included and some of the assumptions that we made while developing the analytical model, such as those on infinite buffer capacity or on the data generation process at the network nodes, can be modified. Furthermore, we point out that the model can be extended to describe various aspects in the design of sensor networks, such as data aggregation or backpressure traffic mechanisms. Finally, cluster-based network architectures as well as the case where the network topology varies because some of the sensors run out of energy and die, could be studied.

6. References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “A Survey on Sensor Networks”, IEEE Comm. Mag., Aug.
2002, pp. 102–114.
[2] S. Singh, C. S. Raghavendra,“PAMAS: Power Aware Multi-Access Protocol with Signaling for Ad-Hoc Networks”, ACM Computer Communication Review, July 1998, pp. 5–26.
[3] W. Ye, J. Heidemann, D. Estrin,“An Energy Efficient MAC Protocol for Wireless Sensor Networks”, IEEE Infocom, New York, NY, June 2002.
[4] C. Intanagonwiwat, R. Govindan, D. Estrin,“Direct Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks”, IEEE/ACM MobiCom 2000, Boston, MA, Aug. 2000.
[5] R. Jain, A. Puri, R. Sengupta,“Geographical Routing for Wireless Ad-Hoc Networks Using Partial Information”, IEEE Personal Comm. Feb. 2001.
[6] B. Chen, K. Jamieson, H. Balakrishnan, R. Morris, “Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad-Hoc Wireless Networks”, IEEE/ACM MobiCom, Rome, Italy, July 2001.
[7] J. Kulik, W. Rabiner Heinzelman, H. Balakrishnan, “Negotiationbased Protocols for Disseminating Information in Wireless Sensor Networks", ACM/IEEE MobiCom ’99, Seattle, WA, Aug. 1999.

[8] F. Ye, H. Luo, J. Cheng, S. Lu, L. Zhang,"A Two-tier Data Dissemination Model for Large-scale Wireless Sensor Networks", ACM/IEEE MobiCom 2002, Atlanta, GA, Sep. 2002.
[9] C. Florens, R.McEliece,"Packet Distribution Algorithms for Sensor Networks", IEEE Infocom, San Francisco, CA, Mar. 2003.
[10] A. Sinha, A. P. Chandrakasan,"Dynamic Power Management in Wireless Sensor Networks", IEEE Design and Test of Computers Magazine, Vol. 18, No. 2, Mar.-Apr. 2001, pp.
62–74.
[11] C. Schurgers, V. Tsiatsis, S. Ganeriwal, M. Srivastava, "Topology Management for Sensor Networks: Exploiting Latency and Density," 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2002.
[12] R. Zheng, J. Hou, L. Sha,"Asynchronous Wakeup for Power Management in Ad Hoc Networks", MobiHoc 2003, Annapolis, MD, June 2003.
[13] P. Gupta, P. R.Kumar,"The Capacity of Wireless Networks," IEEE Trans. on Information Theory, Vol. 46, Mar. 2000.
[14] S. Shakkottai, R. Srikant, N.B. Shroff,"Unreliable Sensor Grids: Coverage, Connectivity and Diameter", IEEE INFOCOM, San Francisco, CA, Apr. 2003.
[15] A. F. Mini, B. Nath, A. A. F. Loureiro,"A Probabilistic Approach to Predict the Energy Consumption in Wireless Sensor Networks", 4th Workshop de Comunicao sem Fio e Computao Mvel, So Paulo, Brazil, Oct. 2002.
[16] A. Ephremides,"Energy Concerns inWireless Networks", IEEE Wireless Communications, Aug. 2002.
[17] D. B. Johnson, D.A. Maltz,"Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, Imielinski and Korth, Eds., Vol. 353, Kluwer Academic Publishers, 1996.
[18] W. Rabiner Heinzelman, A. Chandrakasan, H.Balakrishnan,"Energy-Efficient Communication Protocol for Wireless Microsensor Networks", 33rd International Conference on System Sciences (HICSS '00), Jan. 2000.

V.Shanmukha Rao is currently working as an Associate Professor,Andhra Loyola Institute of Engineering & Technology, Loyola College Campus, Vijayawada. He completed his masters degree from AMA college of Engineering, Madras University and he was also awarded M.Tech (Computer Science) and M.Phil (Computer Science) degrees. He started his career since 2001and offered his services in various institutions, and he also worked as a HOD of IT in Olympia College, Raffles Education Group, Malaysia. He supervised several research projects for MCA, M.Tech and M.Phil students.

Aparna Allada Worked as Assistant professor at various colleges and currently working as Associate Professor in the department of Computer Science at SWARNANDHRA ENGINEERING COLLEGE, Narsapur.Has 9 yrs expirience in teaching field and is the member of IETE.

Sk.Ahmad Mohiddin has completed his M.Tech in Information Technology from JNTU, Kakinada. His research interest includes Data Mining and Data Warehousing, Information Security, Software Engineering etc. He worked with Jogaiah Institute of Technology and Sciences, Palakol. He is currently working as Associate Professor, SwarnandhraEngineeringCollege, NARSAPUR.