



Study on Authentication and Routing Protocols for Secure and Efficient Data Transmission in CWSn

Payal Machirkar, Nita Thakare, Animesh Tayal

Department of Computer technology
PCE, Nagpur, India

Abstract—In Wireless Sensor Networks (WSNs), authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate DoS attacks exploiting the limited resources of sensor nodes. Wireless sensor networks are ad-hoc networks comprised mainly of small sensor nodes with limited resources, and are rapidly emerging as a technology for large-scale, low-cost, automated sensing and monitoring of different environments of interest. Cluster-based communication has been proposed for these networks for various reasons such as scalability, low cost and energy efficiency. In this paper, we investigate the problem of adding security to cluster-based communication protocols for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources, and propose a security solution for the network, a protocol where clusters are formed dynamically and periodically. With the same we are going to discuss about the energy efficiency of the cluster based system while transferring the data or information through cwsns.

Keywords— online/offline signature scheme, public key scheme, energy consumption model, routing protocol, ADVR protocol

I. INTRODUCTION

A wireless sensor network (wsn) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a wsn [1]. Efficient data transmission is one of the most important issues for wsns. Meanwhile, many wsns are deployed in harsh, neglected, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2]. Cluster-based communication protocols have been proposed for ad hoc networks in general and sensor networks in particular for various reasons including scalability and energy efficiency. In cluster-based networks, nodes are organized into clusters, with cluster heads (chs) relaying messages from ordinary nodes in the cluster to the base station (bss) [3]. Adding security to wsns is specially challenging. Existing solutions for conventional and even other wireless ad hoc networks are not applicable here, given the lack of resources in sensor nodes. Public-key-based methods are one such example. In addition, efficient solutions can be achieved only if tailored to particular network organizations. In this paper, we investigate the problem of adding security to cluster-based communication protocols for homogeneous wsns (those in which all nodes in the network, except the bss, have comparable capabilities) and about the energy efficiency of the cwsns.

II. RELATED WORK

The number of literatures specifically targeted to security of WSNs has grown significantly. Here, we discuss about the studies based on cryptographic methods, and focus on those targeted to access control for WSN. Guilin Wang [4] focused on adding security to cluster-based communication protocols in homogeneous WSNs. Cryptography and Online/Offline Signature (OOS) schemes, comprised of two authentication schemes; one for quick authenticated broadcast/multicast by sensor nodes and another for outside user authentication. The first scheme allows every sensor node in the network to broadcast or multicast authenticated messages very quickly without the involvement of the base station. All potential receivers can verify a message sent by any sender node in the network. It also allows sensor nodes on the path from the sender node to the receivers to verify a valid message and drop false injected data. The second scheme enables all sensor nodes in the network to verify the legitimacy of any outside user without storing user specific information. It allows a maximum possible number of legitimate users to access data from sensor nodes in a secure way. This scheme first authenticates a user and then establishes a session key for secure exchange of user queries and sensor nodes data [4].

Table I
COMPARISON OF PROPOSED BROADCAST AUTHENTICATION SCHEME WITH EXISTING BROADCAST AUTHENTICATION SCHEMES.

| Schemes | Signature Scheme | Energy Cost (Offline) mWs | Energy Cost (Online) mWs | Computation Time (Online) s | Storage Overhead (KB) | Message Size (bytes) |
|--|------------------|---------------------------|--------------------------|-----------------------------|-----------------------|----------------------|
| Existing Broadcast Authentication Schemes | | | | | | |
| CAS [24] | ECDSA | 0 | 26.96 | 0.89 | 0 | 148 |
| DAS [24] | ECDSA | 0 | 26.96 | 0.89 | (0.022N ⇒) 1441 | 84 |
| IDS [23] | Pairing based | 0 | 87.09 | 3.47 | 0 | 108 [24] |
| IMBAS [6] | BNN [2] | 0 | 72.90 | 2.43 | 0 | 107 |
| Proposed Broadcast Authentication Scheme | | | | | | |
| Proposed | IBOOS [25] | τ^* | 5.62 | 0.19 | 0 | $64 + \rho^*$ |
| Proposed | IBOOS [31] | 48.60 | ϵ^* | ϵ^* | 0 | 84 |

τ^* and ρ^* show the computational cost and the signature size of underlying signature scheme respectively and ϵ^* shows negligible cost

Shamir introduced the idea of identity(ID)-based public key cryptosystem, which enables any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted key generation center issues a private key to each user when he first joins the network.

Zhou Ruyan, Chen Ming et al. introduces the the cluster-based routing protocols for wireless sensor network based on genetic clustering algorithm. In the network of non-uniform distribution nodes, this method can select the cluster heads after setting the nodes. During the operation of the WSN, when the geographic location change or failure of cluster heads, WSN need to be re-cluster or reselecting the cluster heads, the method proposed in the paper can be used. By using this method, the scientific and rational treatment results can be gotten, which has important practical significance in balancing the network energy and extending the network life cycle[5].

P. Nuir et al [6] presented an Energy-efficient and Secure Pattern-based Data Aggregation protocol (ESPDA) for wireless sensor networks. ESPDA was energy and bandwidth efficient because cluster-heads prevent the transmission of redundant data from sensor nodes. ESPDA was also secure because it does not require the encrypted data to be decrypted by cluster-heads to perform data aggregation. In ESPDA, cluster-head first requests sensor nodes to send the corresponding pattern code for the sensed data. If multiple sensor nodes send the same pattern code to the cluster-head, then only one of them is permitted to send the data to the cluster-head. Hence, ESPDA has advantages over the conventional data aggregation techniques with respect to energy, bandwidth efficiency and security. Simulations results show that as data redundancy increases, the amount of data transmitted from sensor nodes to cluster-head decreases up to 45% when compared to conventional algorithms.

María Gabriela Calle Torres has focused on energy consumption rate for sensors in a wireless sensor network which varies greatly based on the protocols the sensors use for communications. The Gossip- Based Sleep Protocol (GSP) implements routing and some MAC functions in an energy conserving manner. The effectiveness of GSP has already been demonstrated via simulation. However, no prototype system has been previously developed. GSP was implemented on the Mica2 platform and measurements were conducted to determine the improvement in network lifetime. Results for energy consumption, transmitted and received power, minimum voltage supply required for operation, effect of transmission power on energy consumption, and different methods for measuring lifetime of a sensor node are presented. The behaviour of sensor nodes when they are close to their end of lifetime is described and analyzed[7].

III. ENERGY CONSUMPTION MODELS

3.1 The classical energy consumption model

Heinzelman et. al proposed an energy consumption model for sensors based on the observation that the energy consumption would likely be dominated by the data communications subsystem [8]. Table 2.1 reproduces their model.

Table :- radio characteristics, classical model

| Radio mode | Energy Consumption |
|--|---------------------|
| Transmitter Electronics ($E_{Tx-elec}$) | $50nJ / bit$ |
| Receiver Electronics ($E_{Rx-elec}$) | |
| ($E_{Tx-elec} = E_{Rx-elec} = E_{elec}$) | |
| Transmit Amplifier (\mathcal{E}_{amp}) | $100pJ / bit / m^2$ |
| Idle (E_{idle}) | $40nJ / bit$ |
| Sleep | 0 |

The model considers a low power consumption radio that was slightly better than some standard definitions, like Bluetooth [24]. The model provides a commonly used starting point, however, the model has not been verified against the behavior of a physical radio in a wireless sensor network. When computing node energy consumption, the CPU and the sensors are consumers that may or may not be neglected, depending on the nature of the application. So, the radio model must be used jointly with some figure of the energy consumption of those elements, because in the end, power supply must feed all the system and not just the radio.

3.2. Mica2 Specific Model

Polastre et. al proposed a model that presents the total energy consumption for Mica2 as the summation of energy transmitting, receiving, listening, sampling data and sleeping [9]. Values are calculated using the expected consumption of the CPU and the radio, which can be found in specific datasheets [27]. Table 2.3 presents a summary of current consumption.

Table:-current consumption for mica 2 model

| Operation | Time (s) | | I (mA) | |
|---------------------------|----------|-------------|--------|-------------|
| | | | | |
| Initialize radio (b) | 350E-6 | t_{rinit} | 6 | c_{rinit} |
| Turn on radio (c) | 1.5E-3 | t_{ron} | 1 | c_{ron} |
| Switch to RX/TX (d) | 250E-6 | $t_{rx/tx}$ | 15 | $c_{rx/tx}$ |
| Time to sample radio (e) | 350E-6 | t_{sr} | 15 | c_{sr} |
| Evaluate radio sample (f) | 100E-6 | t_{ev} | 6 | c_{ev} |
| Receive 1 byte | 416E-6 | t_{rxb} | 15 | c_{rxb} |
| Transmit 1 byte | 416E-6 | t_{txb} | 20 | c_{txb} |
| Sample sensors | 1.1 | t_{data} | 20 | c_{data} |

As the authors present current consumption and time, and assuming that Mica2 is powered by a 3V source [2], one can calculate energy in transmitting and receiving one bit, as:

$$Energy = Current * Voltage * Time \quad (2.5)$$

Where current is in Amperes, Voltage is in Volts and Time is in seconds.

$$Energy_{Tx} = 20 * 10^{-3} \text{ A} * 3 \text{ Volts} * 416 * 10^{-6} \text{ sec} / 8 \text{ bits} = 3.12 \mu\text{J/bit} \quad (2.6)$$

$$Energy_{Rx} = 15 * 10^{-3} \text{ A} * 3 \text{ Volts} * 416 * 10^{-6} \text{ sec} / 8 \text{ bits} = 2.34 \mu\text{J/bit} \quad (2.7)$$

The difference with the Heinzelman model is two orders of magnitude [24]. With the μ AMPS model, energy for transmission is comparable, while energy for reception is one order of magnitude bigger in the Mica2 case.

This are the various energy model were used for energy consumption in cluster based wireless sensors network. And the other energy models has been proposed later.

IV. ROUTING PROTOCOLS FOR SENSOR NETWORKS

There are several routing protocols proposed for sensor networks. GSP, the routing protocol used in this experiment, is based on the Flooding concept.

4.1 Flooding:

Flooding is a method where every packet received is retransmitted to all the nodes in the network [20]. Variations include only retransmitting the packet if it has not reached a maximum number of hops or if the destination node is the node itself [3]. In order to know this, some kind of addressing scheme must be used. Flooding is a simple algorithm, but it has several disadvantages when used in sensor networks [21]:

- Implosion: duplicated messages are sent to the same nodes.
- Overlap: If two nodes are in the same region, they may sense the same signal at the same time and transmit the same information twice.
- Resource blindness: The Flooding method does not depend on whether energy resources are scarce or not. The method works the same in any of the two situations.

Figure 4.1 illustrates an example network. Nodes B and C can listen to A and vice versa. Node D is in range of C and B only. When node A sends a packet, nodes B and D receive it and they retransmit it. As A is in the same range, it will hear again the same packet that it sent, and it will retransmit the same packet. The packet eventually will propagate through the whole network, but there will be a big amount of duplicate packets, if no improvements are applied to the algorithm.

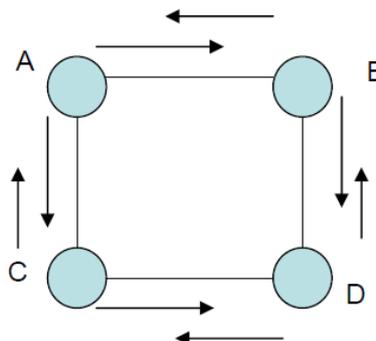


Figure 4.1 Flooding Algorithm example

4.2 Gossiping

The method tries to improve the flooding algorithm by the following procedure: the nodes have a probability p of broadcasting the packet they receive. With probability $1-p$, the received packet is discarded [11]. Gossiping avoids the implosion problem, but the time it takes for the packet to get to the destination is long, according to [12]. There are no synchronization requirements [12]. As an example, a similar network as before is presented in Figure 2.8. In this case, node A transmits a packet. With probability p , B retransmits the packet and with probability $1-p$ C drops the packet. When the packet gets to D, the coin is tossed again and the packet in this figure is sent again. Notice that C spent energy receiving the packet that would be dropped, according to $1-p$.

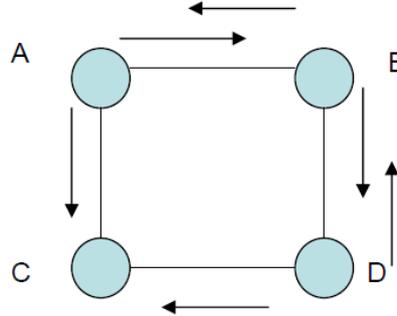


Figure 4.2 Gossiping example

4.3 GSP: Gossip-based Sleep Protocol for Energy Efficient Routing in Wireless Sensor Networks

GSP uses a duty cycle for the transmission. In one part of the duty cycle, the radio is on, so the node can transmit and receive. With a probability p , the radio will be off in the next part of the duty cycle, so the node will not be able to transmit or receive any packet. When a node receives a packet, it must retransmit it. Figure 4.3 illustrates an example network employing GSP. In this case, A sends a packet. Assuming that B has its radio on and C its radio off, B will receive the packet and will retransmit the packet. C did not spend energy in receiving the packet. D will receive the packet only if its radio is on. In that case, it will retransmit the packet.

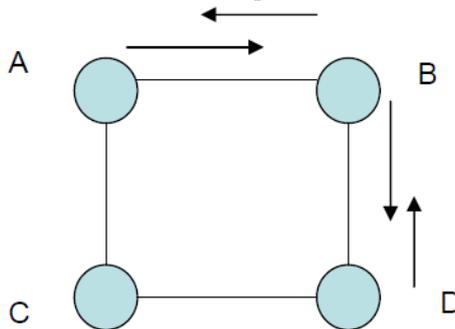
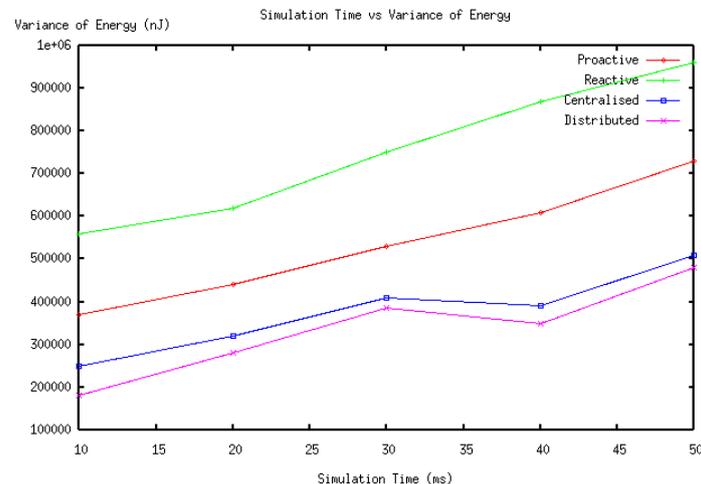


Figure 4.3 GSP algorithm example

4.4 Advanced distance vector routing protocol (ADVR)

Now we have discussed about ADVR protocol which uses all the mobile nodes to form cluster. By using this routing protocol each node will be in cluster of 1 or 2 and the data transmission path will become longer and the process will be faster. As more amount of data will be transmitted the nodes lifetime will be increased and more energy will be saved because of less traffic and low data loss. Comparison with other routing protocols has been shown below in graph.



ACKNOWLEDGEMENT

In this paper we studied the different techniques for secured data transmission using the clustered based wireless sensor network and different routing protocols for energy efficiency. Clustered based sensor network has been proposed for the ad-hoc network. In this study the idea getting for an efficient and secured transmission of data. We have discussed about the various routing protocols in order to increase the lifetime of the nodes. So in the future work we will implement the network with an efficient time and space constraining algorithm and a technique to transmit more data in less traffic and faster transmission.

REFERENCES

- [1] T. Hara, V.I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
- [2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Comm. Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
- [3] Adrian Carlos Ferreira¹, Marcos Aur elio V ila ç a¹, Leonardo B. Oliveira¹, Eduardo Habib¹, Hao Chi Wong¹, Antonio A.Loureiro¹, "On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks", Federal University of Minas Gerais, MG, Brazil.
- [4] An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures Rehana Yasmin, Eike Ritter, Guilin Wang Dept. of Computer Science University of Birmingham, B15 2TT Birmingham, United Kingdom Email: fR.Yasmin, E.Ritter, G.Wangg@cs.bham.ac.uk W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," presented at National Computer Conference, New York, June 7-10, 1976.
- [5] Zhou Ruyan, Chen Ming, Feng Guofu, Liu Huifang, He Shijun, "Genetic Clustering Route Algorithm in WSN", 2010 Sixth International Conference on Natural Computation (ICNC 2010), 978-1-4244-5961-2/10/\$26.00 ©2010 IEEE. NETWORKS", 0-7803-813 3-5/03/\$17.0002 003 IEEE.
- [6] H. cum, S. Ozdemir, P. Nuir*, D. Muthuavinashiappun, "ESPDA: ENERGY-EFFICIENT AND SECURE PATTERNBASED DATA AGGREGATION FOR WIRELESS SENSOR
- [7] ENERGY CONSUMPTION IN WIRELESS SENSOR NETWORKS USING GSP University of Pittsburgh 2006 Submitted to the Graduate Faculty of the School of Information Sciences in partial fulfillment of the Master of Science in Telecommunications by **María Gabriela Calle Torres** Electronics Engineer, Universidad Pontificia Bolivariana, Medellín, Colombia, 1995
- [8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks" in *IEEE Hawaii International Conference on Systems Sciences*, 2000.
- [9] J. Chang, L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks", *IEEE INFOCOM*, Tel Aviv, Israel, 2000.
- [10] V. Shnayder, M. Hempstead, B. Chen, G. Werner Allen, and M. Welsh, "Simulating the Power Consumption of Large Scale Sensor Network Applications", *SenSys'04*, Baltimore, Maryland, USA, November 3-5, 2004.
- [11]. Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing," in *Proceedings of IEEE INFOCOM*, 2002.
- [12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. "A Survey on Sensor Networks", *IEEE Communications Magazine*, August 2002.
- [13] Zhou Ruyan, Chen Ming, Feng Guofu, Liu Huifang, He Shijun, "Genetic Clustering Route Algorithm in WSN", 2010 Sixth International Conference on Natural Computation (ICNC 2010), 978-1-4244-5961-2/10/\$26.00 ©2010 IEEE
- [14] Vishnu Kumar, Yunjung Park, Dugki Min, Eunmi Choi, "Secure-EEDR: Dynamic key exchange protocol based on Diffie-Hellman algorithm with NOVSF code-hopping technique for wireless sensor networks", 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering .
- [15] I-Hsun Chuang¹, Wei-Tsung Su¹, Chun-Yi Wu², Jang-Pong Hsu², Yau-Hwang Kuo¹, "Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks", This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings, 1525-3511/07/\$25.00 ©2007 IEEE.