Secure Communication and Routing Architecture in Wireless Sensor Networks

Abdelali EL BOUCHTI, Abdelkrim HAQIQ
Computer, Networks, Mobility and Modeling laboratory
e-NGN Research Group, Africa and Middle East
FST, Hassan 1st University, Settat, Morocco
{a.elbouchti, ahaqiq}@gmail.com

ABSTRACT**:** *Security of wireless sensor networks (WSN) is an important feature, as they are used in critical applications such as surveillance, monitoring, tracking and controlling etc. Secure and reliable communication is highly important in delivering critical information correctly and in-time by low-powered sensor motes (SM). Many secure WSNs protocols have been proposed but they have focused primarily on denial-of-communication at the routing or medium access control levels. Although WSNs have interesting distinctiveness (i.e., minimum set-up cost, unattended network operation), and because of the wireless medium (i.e., there are no gateways or routers to observe data flow), the security of these networks is the main issue, particularly when privacy is the main theme. Secure communication in WSNs reclines in the security of their routing protocols. However, resource bound security solutions are needed for WSNs. This paper has proposed novel security mechanism by combining features of two security architectures in WSNs, i.e., TESLA from SPINE and Bloom Filters (BF) from MiniSec. We have used TOSSIM for simulation and showed that our proposed mechanism perform better than other security schemes.*

Keywords: Wireless Sensor Networks, TESLA & Bloom Filters, Routing Protocols, Secure Communication Architecture

Received: 12 February 2014, Revised 29 March 2014, Accepted 14 April 2014

1. Introduction

WSN is a web of tiny SM, and usually they are neither replaceable nor rechargeable. A SM consists of sensing, processing, power, and communication units, but these units have limited capabilitie. A WSN is used in diverse ubiquitous and pervasive applications such as military, security, health-care, industry automation, environmental and habitat monitoring [1].

There is a vast varity of different hindrances in WSN, and security is an important glitch due to various resource restrictions. A design of secure WSN is considerably tricky, as SM have rigorous resource restrictions, such as limited processing, memory and power. Therefore, conventional security architectures with bulky overhead of processing, routing, and communication are infeasible in WSNs.

In fact, offering security in SM is hard due its limited hardware. Using wireless medium and the unattended characteristics of WSN make it easy to eavesdropping, infusing malicious data, whereas, low power, processing, & energy of WSNs make them vulnerable to DoS attacks. Mostly security architectures are intended for limited motes and do not fit to a large number of SM. Large scale deployments need to be considered.

In this paper a secure communication and routing mechanism in WSN has been proposed, which primarily focuses on three major issues. Our first concern is to achieve secure communication with limited resources, by introducing hybrid architecture. Second point of concern is to avoid intrusion detection by introducing multipaths between sender and receiver. Third issue need to be resolved is broadcast authentication (BA) and protection from replay.

The rest of this paper is structured as follows. In the next section, the related work is reviewed, and Section III discuses system model, system assumptions and routing attacks; detailed description of the proposed mechanism is provided in Section IV. Section V presents simulation results and Section VI concludes the paper.

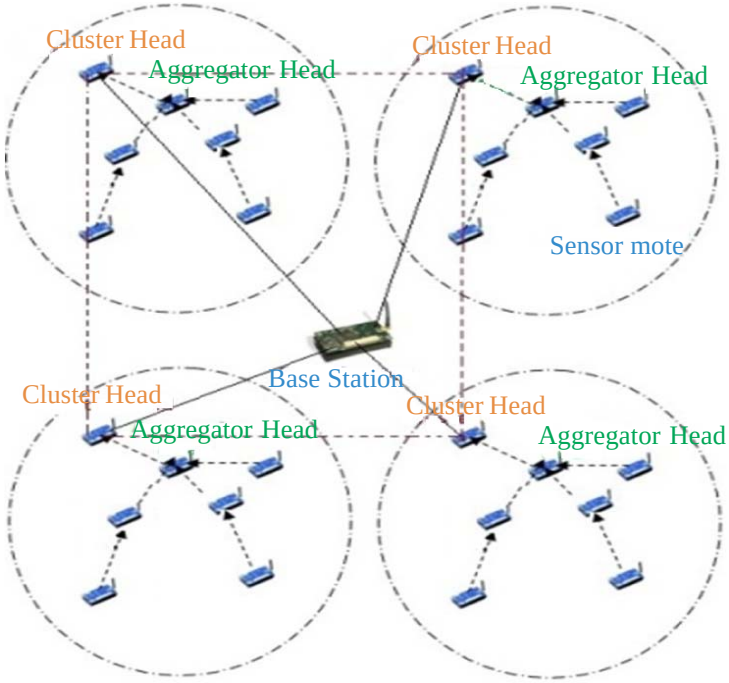

Figure 1. Network Model

Layer	Attacks	Security Approach
Physical	Jamming & Tampering	Use spread spectrum techniques and medium access control layer admission control mechanisms
Datalink	Jamming & Collision	Use error correcting codes and spread spectrum techniques
Network	Sinkhole	Redundancy checking
	Sybil	Authentication, Monitoring
	Wormhole	Authentication, probing
	Hello flood	Authentication, packet leashes by geographical and temporal information
Transport	Injects false messages and energy drain attacks	Authencation
	Flooding	Client puzzles
	De-synchronization	Authencation
Application	Attacks on reliablity	Cryptographic approach

Table 1. Layer-wise Attacks and Possible Security Approach

Algorithm 1 for discovering neighbor nodes

1 CH_x: Route Request (Id_{Lx})

2 SM_y: adds the Id CH_x to neighbors List

3 SM_y: Route Request appending its own identity (Id_{Lx}, Id_{Ly}....) (But for the first time only)

4 SM_y: Repeat step-2 for each Route Request Message

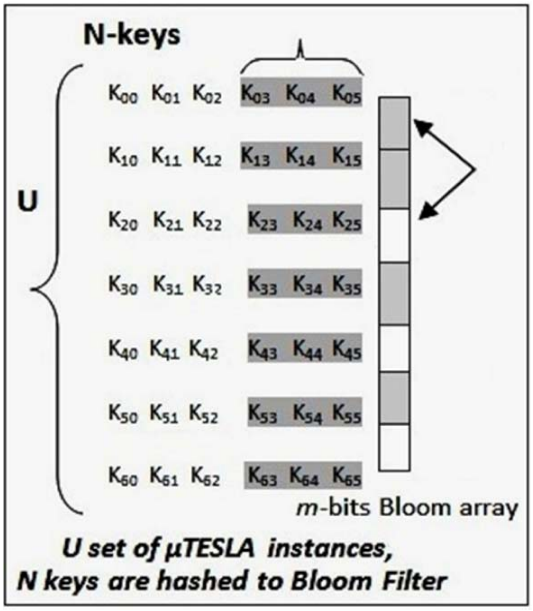

Figure 2. set of μ TESLA instances and hashed Keys

2. Related Work

In resource constrained WSNs, routing is a hard area. Geographic routing has been broadly considered as one the most impressive technique for WSNs. These protocols exploit geographic information to route data packet in multihop WSNs [2]. The sender selects neighbors for data-forwarding based on direction or distance [3, 4]. The distance between nodes can be calculated by signal-strength [5, 6]. In [7], trust & reputation metrics are calculated by SMs for their neighbors, and if a SM finds shared information erroneous, the mote is judged as malicious and adequate action is taken against the subject malicious mote. The working of SM is managed by adopting various rules on the motes. These rules consist of security and confidentiality that find integrity, BA, encryption/decryption, etc. Numerous attacks may be initiated by malicious motes on these rules such as, excuse attack, newbie-picking attack [8] etc.

In [9] probabilistic routing has been proposed for enhancement of link reliability and residual energy. We have proposed a energy efficient clustering scheme in WSNs [1], and performance improvement in adhoc networks [11,12], whereas our work on cognitive radio networks is published in [13]. In addition, a probabilistic key-management technique in WSN has been studied in [14], which uses pair-wise key and is useable in numerous application. Similarly in [15], keymanagement techniques are proposed but their agility against node capture attacks in weak. However, their suggested Bloms algorithm achieves better results against the same attacks. Bloms key-distribution mechanism offers a better connectivity in a shorter transmission range and lower memory requirement.

In literature, a number of security protocols and architecture have been studied, such as ARRIVE [10], INSENS [20], TinySec [21], SPINE [22], MiniSec [23], FlexiSec [24]. SPINE uses TESLA for BA, whereas MiniSec uses Bloom Filter (BF) for rate control and replay protection. Our proposed mechanism is a combination of TESLA and BF for secure BA, route formatin with low energy consumption & computation costs. Moreover, some good survey on WSN security, attacks and countermeasure have been studied in [16-19].

Parameters	Values
Field	$[200 \times 200]$
BS location	[125, 90]
Protocol Used	INSENS, Proposed Mechanism
Number of nodes	20
Packet Size	36Bytes

Table 1. Simulation Conditions

3. Network Model and System Assumptions

The network has a BS installed in the center of the network with high power and processing capabilities. For load balancing, all clusters have CHs and Aggregator Heads (AH) as in [1]. The network model is shown in Figure 1, and assumptions of our network model and some routing attacks on WSN are discussed below.

The assumptions made are all SMs are unique, stationary, equipped with tamper resistant hardware, and calculate distance by signal-strength. CHs directly communicate with each other, and are loaded with unique secret key set by BS. In addition, CHs share these keys with their SMs in their respective clusters via AH.

SMs employ shared pair-wise keys for BA between CHs & SMs. Further, SMs are pre-loaded with BFs, with hashed TESLA instances needed for one-way BA. SMs communicate with each other after sharing pair-wise keys. SM can be hacked at route formation or routing table creation stage, but adversary may get control of only one secret key and not the secret keys of entire network, therefore, may get access cryptographic data stored on a SM. SM routes information to the AH using multi-hops and multipaths. Moreover, adversary can launch different attacks on WSN; and a list of layer-wise attacks and their countermeasures is depicted in Table 1.

4. Proposed Method

The proposed mechanism embeds security architecture in the design of routing protocol, instead of making separate protocol for efficient routing & intrusion detection. The proposed mechanism is a three step process: *cluster formation*, *rout formation* and *data forwarding*. The first step is same as in [1], which reduces energy consumption in network initialization. The first step elects the CH and selects AH. In route formation phase, routing tables are created, and all SMs forward their topology information to CH through route response message via AH. The CH generates pair-wise keys for SMs, send them via AH, and use Algorithm-1 for identifying neighbor nodes and to accommodate changes in topology. Before data forwarding phase, AH is selected and

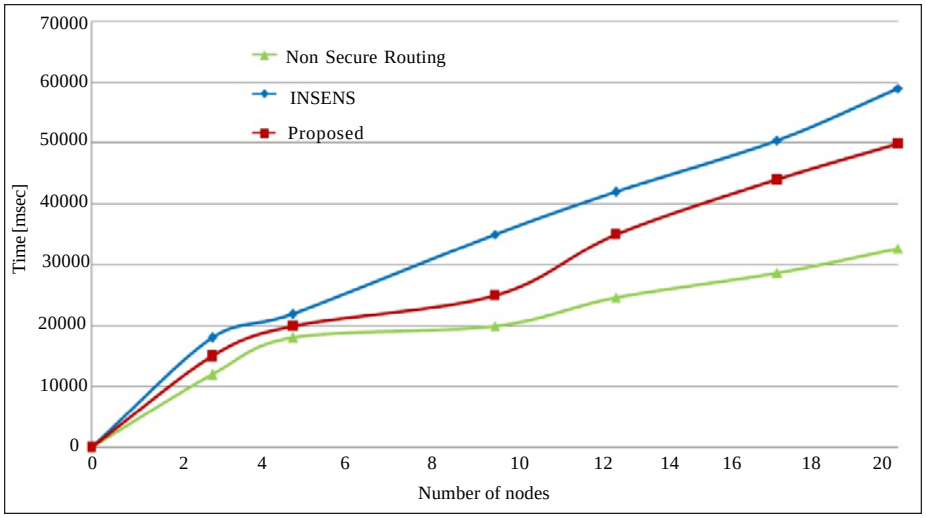

Figure 3. Network Setup Time

multipath are discovered. SMs forward data in multihops/multipaths using routing tables with pair-wise keys shared by CH, these keys jelp in maintaining data integrity. Data is forwarded on all available routes; to avoid data from jamming, selective forwarding, or sinkhole attacks; whereas TESLA and BFs provides BA and replay protection. Figure 2 shows set of TESLA instances, where N keys are hashed to BF.

4.1 Network Setup Time

The network setup time is the interval between network initialization till exchange of routing tables. This time consists of, RC5 execution, packet processing, and delay for route response message. Figure 3 shows that our proposed mechanism performs better than INSENS. However, Non- Secure Routing (NSR) takes less time as they do not need encryption/decryption.

4.2 Communication Overhead

The communication overhead is shown in Figure 4. The proposed mechanism has less overhead compared to INSENS, whereas NSR performs better due to less computation by SMs, i.e., no execution of extra code for security. The reason is that the proposed mechanism appends last 64-bits of calculated MAC into the packets, and more processing is done locally at the AH.

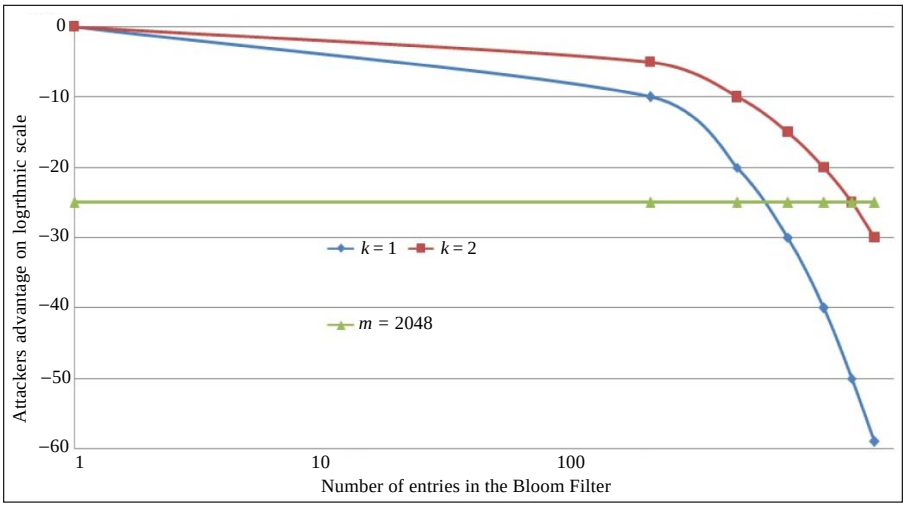

Figure 4. Communicatioin Overhead

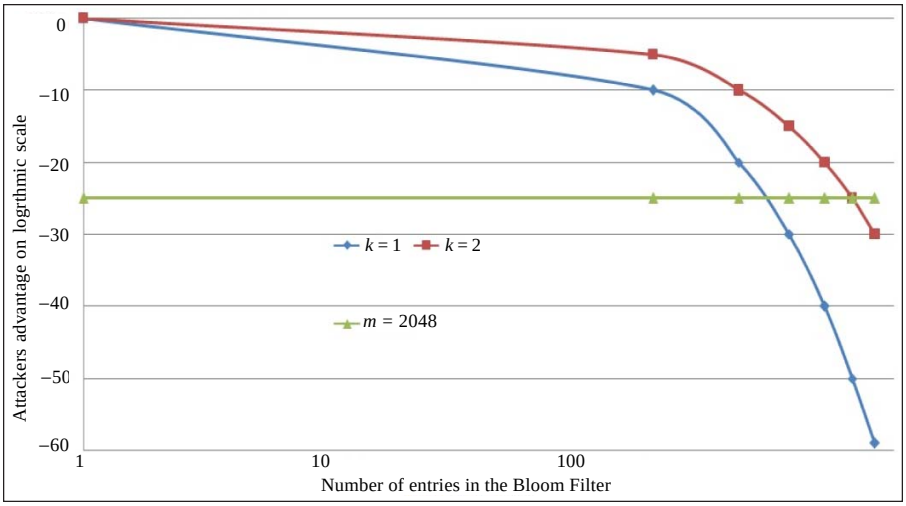

Figure 5. Attacker Success Rate

4.3 Broadcast Authentication

For the privacy of data; packets are encrypted using RC5, which is default encryption/decryption tool in TinyOS. The success ratio of an attacker against the proposed mechanism is depicted in Figure 5. The number of entries in the BF is inversely

proportional to the success ratio of an attacker. If we use a Compressed BF our scheme will perform even more better.

6. Conclusion

This paper has presented a novel secure routing mechanism in WSN with BA using TESLA & BF. BA is helpful in hoarding against compromised nodes, whereas multipath routing avoid jamming of network. Simulation results show that proposed mechanism is vigorous against numerous routing attacks.

References

[1] Khan, F., Bashir, F., Nakagawa, K. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks *in the IEEE International Conference of Emerging Technologies, Islamabad, Pakistan,* p. 8-9, *October.*

[2] Li, Y., Li, J., Ren, J., Wu, J. (2012). Providing hop-by-hop authentication and source privacy in wireless sensor networks, *in IEEE INFOCOM, Mini-Conference,* Orlando, Florida, USA., March, p. 25-30.

[3] Barani, S. (2012). Energy Aware Routing Algorithm for Wireless Sensor Networks, *in Indian Journal of Computer Science and Engineering,* 2 (6), ISSN: 0976-5166.

[4] Radi, M., Dezfouli, B., AbuBakar, K., Lee, M. (2012). Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges *in Sensors*, 12, p. 650-685.

[5] Han, G., Xu, H., Doung, T. Q., Jiang, J., Hara, T. (2013). Localization Algorithm forWireless Sensor networks: a survey *in Telecommunication System*, 52 (4) 2419-2436.

[6] Tie-zhou, W., Yi-shi, Z., Hui-jun, Z., Biao, L. (2013). Wireless Sensor Network Node Location based on improved APIT *in the Journal of Surveying and Mapping Engineering*, 1 (1) 15-19.

[7] Sen, J., Bessis, N. (2013). An efficient, secure and user privacy-preserving search protocol for peer-to-peer networks, *Book Chapter in: Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence,* et al. (eds.), p. 279-320, Springer, Heidelberg, Germany.

[8] Araujo, A., Blesa, J., Romero, E., Villanueva, D. (2012). Security in cognitive wireless sensor networks: Challenges and open problems, *in EURASIP Journal on Wireless Communications and Networking,* p. 48.

[9] Hung, C. C., Lin, K.-J., Hsu, C. C., Chou, C. F., Tu, C. J. (2010). On enhancing network-lifetime using opportunistic routing in wireless sensor networks, *In*: Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN), Aug. p. 16.

[10] Karlof, C., Li, Y., Polastre, J. (2002). ARRIVE, *University of California at Berkeley,* Tech. Rep. UCB/CSD-03-1233, May.

[11] Khan, F., Kamal, S. A., Arif, F. (2013). Fairness Improvement in long-chain Multi-hop Wireless Ad hoc Networks *in the* IEEE ICCVE 2013, Las Vegas, USA.

[12] Khan, F. (2014). Fairness and Throughput Improvement in Multi-hop Wireless Ad hoc Networks in the 27th Canadian Conference on Electrical and Computer Engineering, Toronto.

[13] Khan, F., Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks *in IEEE International Conference on WCCIT*.

[14] Al-Haija, Q. A. (2010). Toward secure non-deterministic distributed wireless sensor network using probabilistic key management approaches, *in J. Information Assurance Security*.

[15] Kuchipudi, R., Basha, N. M. J. (2012). A distributed nodes local- ization approach in wireless sensor networks, *in Int. J. Computer. Sci Information Technology,* 3, 3187-3190.

[16] Chowdhury, M., Kader, M. F., Zaman, A. (2013). Security Issues in Wireless Sensor Networks: A Survey *in the International Journal of Future Generation Communication and Networking,* 6 (5) 97-116.

[17] Pooja, Manisha, Y. Singh. (2013). Security Issues and Sybil Attack in Wireless Sensor Networks *in the International Journal of P2P Network Trends and Technology,* 3 (1). ISSN: 2249-2615.

[18] Gupta, H. K Verma., Sangal, A. L. (2013). Security Attacks & Prerequisite for Wireless Sensor Networks *in the Int. Journal of Engineering and Advanced Technology* (*IJEAT*), 2 (5).

[19] Sen, J. (2013). A Survey on Security and Privacy Protocols for Cognitive Wireless Sensor Networks, *Journal of Network and Information Security,* 2 (5).

[20] Deng, J., Han, R., Mishra, S. (2006). Insens: Intrusion-tolerant Routing for Wireless Sensor networks, *in Computer Communications,* 29 (2) 216230.

[21] Luk, M., Mezzour, G., Perrig, A., Gligor, V. (2007). Minisec: a secure sensor network communication architecture, *In*: Proceedings of the 6th International Conference on Information Processing in Sensor Networks, New York, NY, USA: ACM, p. 479488.

[22] Karlof, C., Sastry, N.,Wagner, D. (2004). Tinysec in SenSys 04, *In*: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, New York, NY, USA: ACM Press, p. 162175.

[23] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., Culler, D. E. (2002). SPINS *in Wirel. Netw.,* 8 (5) 521534, September.

[24] Jinwala, D., Patel, D., Dasgupta, K. (2009). FlexiSec: A Configurable Link Layer Security Architecture for Wireless Sensor Networks *in the Journal of Information Assurance and Security,* 4, p. 582-603.