Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 585491, 8 pages
http://dx.doi.org/10.1155/2013/585491

Research Article

Framework for Secure Wireless Communication in Wireless Sensor Networks

Muhammad Usama[1] and Fahad T. Bin Muhaya[1,2]

[1] *Prince Muqrin Chair for IT Security, King Saud University, Riyadh, Saudi Arabia*
[2] *College of Applied Studies and Community Service, King Saud University, P.O. Box 2459, Riyadh, Saudi Arabia*

Correspondence should be addressed to Muhammad Usama; usama.khanzada@hotmail.com

Received 25 March 2013; Revised 11 July 2013; Accepted 13 September 2013

Academic Editor: S. Khan

With large-scale and rapid development in wireless sensor networks (WSNs), there is great demand to adopt security mechanisms for secure wireless communication. WSNs have many fields of applications that are playing an essential role in increasing productivity and reducing cost. The restricted and constrained nature of sensors along with potentially dynamic behavior of WSNs demands the proper implementation of framework for secure communication in order to prevent attacker from illegally accessing or altering the transmission. We proposed a framework for secure wireless communication in WSNs which consists of four modules, that is, redundancy checker, message prioritization mechanism, malicious node verification, and malicious data verification. Detailed results of security and performance analysis have been realized for comparison and evaluation with complete implementation using NS2 network simulator. The proposed framework presents numerous interesting features which proofs acceptable performance for malicious node and data detection in WSNs.

1. Introduction

Recent advances in wireless senor networks (WSNs), which are typically composed of low power, small microprocessors, powerful base stations, and a large number of multifunctional resource-constrained sensor nodes [1, 2], have attracted significant attention from industries and academics and are an interesting topic of continuous research. These resource-constrained devices provide sensing functionality when they are networked together over a wireless medium. The dynamic, self-directed and distributed network environment of sensor devices in WSNs leads them to depend on sensors functionality. In WSNs, all sensor nodes communicate and collaborate for a special purpose and common goal. They can be used to collect and process certain physical information and data from the environment such as mechanical, temperature, light, radiation, and optical readings, to transmit on base stations. These features and characteristics of WSNs enables wide range of applicability in various applications of environment monitoring, logistic and health care applications, military operations, and so forth [3–7]. WSNs can be configured as heterogeneous, homogeneous, hierarchical, or distributed. It depends upon requirements with available hardware and network settings options. For example, the design of hierarchical wireless sensor network depends on the capabilities and functionalities of base station, head, and sensor devices as shown in Figure 1. Sensor devices are mostly used for special purposes and they require less power and processing time. They collect data from deployed environment and transmit to nearest head device. The head device is responsible for collecting and processing data gathered from near sensors and forwarding it to base station. Base station further processes the data gathered from head devices to make it meaningful for other networks. The base stations are more powerful and can process large data. In distributed or any other wireless sensor network, the capabilities and functionality of all sensors and devices are similar as shown in Figure 2.

In many WSNs applications, these systems are deployed in unattended, self-directed, dynamic and hostile environments. In such systems, message broadcast technique is an efficient and common communication practice to multiple users. Similarly, user can join the host network by queries or

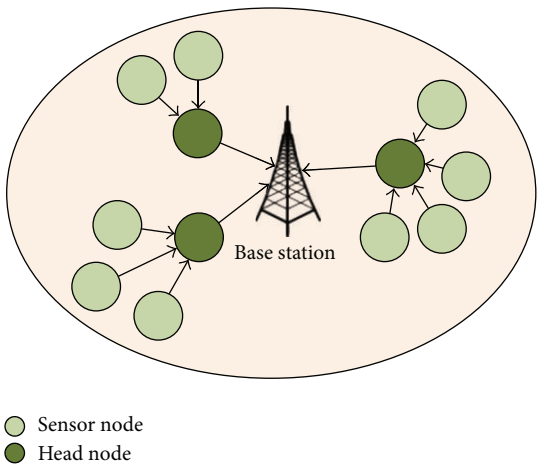


Figure 1: Hierarchical WSNs.

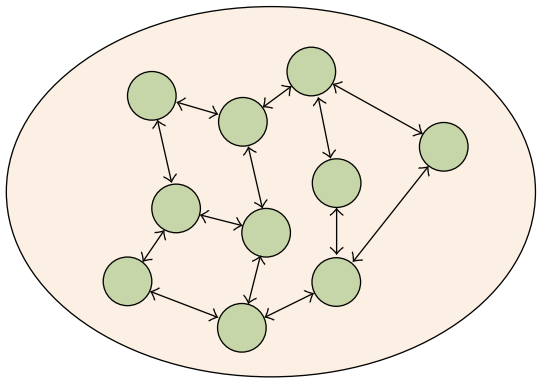


Figure 2: Distributed WSNs.

commands messages for obtaining desired information and data [8, 9]. The use of wireless technology for messages and data transmission requires proper implementation of secure wireless communication framework. Due to the deployment nature and wireless communication, attacker can easily access the transmission, can threaten other users, capture data, and alter or misuse communication illegally. Therefore security becomes serious issue and concern to prevent illegal use or access and protect broadcast messages from various malicious attacks.

In this paper we propose a framework for secure wireless communication to ensure that sensor node communicates secure information to its neighbor through WSN. We evaluate two study scenarios for the broadcast message on WSN to demonstrate the security and performance. The detailed quantitative analysis and experiment show that the proposed framework is greatly superior to the traditional methods and techniques for WSNs in terms of energy consumption and transmission delay of the whole network. It reduces network load using redundancy checker module by removing message redundancy. It is suitable and practical for malicious nodes and detection as compared to existing approaches. Proposed framework supports message prioritization mechanism to ensure more access for network and user traffic as required.

2. Related Work

Many techniques and approaches regarding detection and management of malicious nodes, malicious data, errors, or faults have been published during the last years for secure communication in wireless sensor networks. However, WSNs are susceptible to several security threats and vulnerable to many attacks due to the broadcast nature of data communication. In addition, sensor nodes are more susceptible to attack or danger as they are placed in unattended, self-directed, dynamic, and hostile environments [10]. In [11] Raya and Hubaux presented a security architecture for security and privacy. In [12] Golle et al. proposed a malicious data detection and correction technique based on sensor data and neighbor information. It allows malicious node to perform malicious activities that provides redundant and position information of neighbors in order to detect and correct malicious data. In order to remove malicious nodes, Xiao et al. [13] proposed a scheme based on signal strength that can verify the position to localize and detect. The proposed scheme does not provide acceptable security and comes up with weakness especially against spoof attacks. Again they proposed two static algorithms based on traffic patterns and base stations to overcome the weakness and reduce the effect of malicious nodes.

It is important that system must be able to detect malicious nodes from WSNs with acceptable performance. However, it is difficult to detect malicious nodes due to dynamic nature and lack of proper implementation of WSNs. Many applications suffer because of various security attacks and vulnerabilities, for example, denial of service, malicious node attack, impersonation, copyright and privacy violation, and so forth, due to lack of proper implementation and dynamic nature [14]. Authentication, confidentiality, integrity, and nonrepudiation are also very important and essential security requirements of wireless communication [15]. In denial of service (DoS) attack, attacker attempts to disrupt, subvert, or destroy a network [16]. A DoS attack decrease the network capacity in terms of size, extent, and range in order to reduce network performance from expected functions. Due to the broadcast nature of communication, any attacker can access or use communicated messages and data illegally. Using intrusion or any transmission access techniques, attacker can get important information like location, IDs, timestamps or any specific information, and so forth. WSNs basically adopt neighbor trust model in which sensor nodes rely on neighbor sensor node for message forwarding. In such trust model attacker can exploit communication by selective forwarding attack [17]. Attacker can create malicious node by simply dropping received messages in order to confuse the network transmission that some or all messages are not delivered or dropped. Thus, neighbor should find alternative route for communication, and in the same manners messages can be tampered before forwarding by malicious nodes.

3. Proposed Framework

Generally a secure wireless communication framework requires especial and careful design and implementation that deals with resources constrains while ensuring better

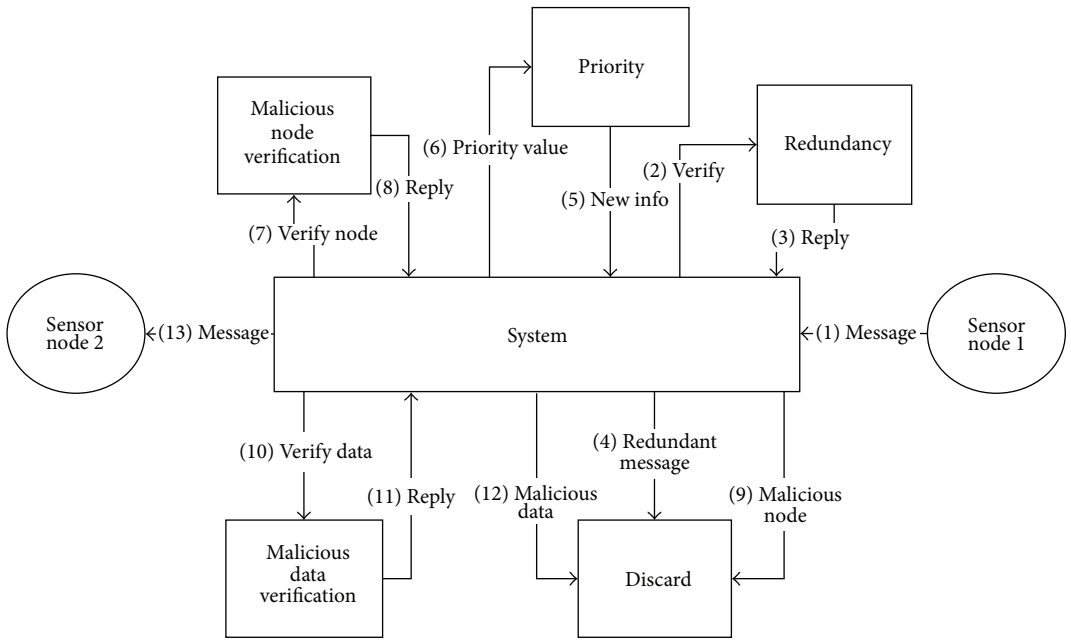


Figure 3: System block diagram.

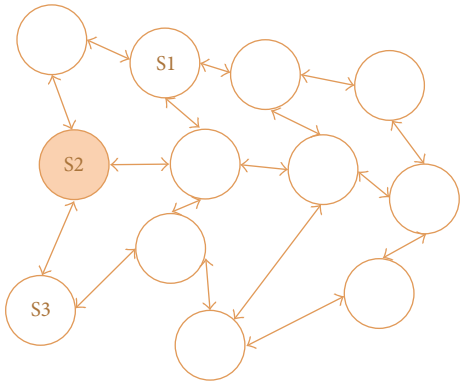


Figure 4: Sensors nodes network where S2 is a malicious sensor node.

performance and efficiency along with flexibility and ease to use application access and processes. In order to provide such a secure framework for WSNs we have made a few reasonable assumptions. We assumed that the base stations and head nodes are secure and attackers cannot access or use them illegally. The proposed framework does not aim any sort of trust assumptions on the wireless communication with the apparent fact of nonzero probability of messages deliveries. Secure communication framework design should build robust and trustworthy system with untrustworthy modules and should have ability to perform well when need arises. Security framework should also work with the same features if change occurs in the system of addition or updating in the network nodes, thus providing scalability with minimum errors.

Our proposed secure wireless communication framework for WSNs is composed of four core modules, called redundancy, message prioritization mechanism, malicious node, and data verification. The block diagram of the proposed framework is given in Figure 3. The system performs the following operation steps in sequential manner in order to ensure secure communication.

Step 1. Sensor 1 wants to share some information with Sensor 2 as message.

Step 2. System sends message to redundancy checker for verification and checking of message redundancy.

Step 3. If the message is redundant than system discard else return for forward. At this stage all redundant messages are discarded and only newly issued messages can be forwarded.

Step 4. System forwards new message for assigning priority value. Priority checker returns back priority value to the system.

Step 5. After performing redundancy checking and priorities for the message, it performs malicious node verification for ensuring security. The malicious node verification module replies to forward the message for further verification or discard.

Step 6. If the node is malicious, then data is discarded; otherwise it returns to system.

Step 7. At the end, the system verifies the message for the presence of malicious data and finally decides to forward the message for further communication or discard.

Step 8. If it is found that message contains malicious data then it is discarded; else it is delivered to neighbor node safely.

Table 1: Simulation parameters.

Parameters	Values
Channel	Wireless
Sensor nodes	N
Protocol	MAC 802.11
Radio propagation model	Two-ray ground
Time	50 seconds
Data	Multimedia

The description of basic functions and assumptions of each module is listed below.

(i) Redundancy checker: in this system, each sensor node is responsible for maintaining unique message ID table of received messages. During communication redundancy checker utilizes the unique message ID to detect or discard the redundant messages.

(ii) Message prioritization mechanism: prioritization mechanism computes and compares the message priority values with other messages. By default, it assigns higher priority to all safety messages.

(iii) Malicious node verification: the malicious node verification process is done using signal strength.

(iv) Malicious data verification: the malicious data verification process is done using existing messages and node position.

4. Implementation and Results

This section will briefly provide an overview on the implementation and results of the proposed framework. Simulations have been performed and observed for multimedia streaming in a wireless sensor network scenario. We assume that the sensor nodes are uniformly distributed and deployed in the field with support of an underlying MAC protocol 802.11 and a two-ray ground model for the wireless channel access. A two-ray ground radio propagation model is used that is an empirical mathematical formulation for the characterization of radio wave propagation [18]. It considers direct and ground paths between two wireless sensor nodes using radio waves propagation. Sensor node can access, channel via MAC protocol after exchanging messages with neighbors. The mobility model is implemented using Manhattan Mobility Model [19]. Multimedia traffic is generated using EvalVid [20]. We perform data availability test by measuring time that elapses to send and receive data traffic to ensure data availability for all network nodes. Detailed simulation results of security and performance analysis have been realized for comparison and evaluation with complete implementation using NS-2 [21] on Cygwin [22]. Experiment control parameters with values used in simulation are given in Table 1.

The performance of the proposed framework highly depends on proper implementation and deployment of WSNs. To analyze the performance of the proposed framework, we conduct two studies to verify the secure wireless communication in WSNs and simulate the data traffic and compute throughput, delay, and PSNR for comparison and evaluation.

(i) Throughput: in a random network that consists of N nodes where each node S has a randomly chosen destination node D and can transmit at t bits-per-second, throughput is scaled as

$$\Theta\left(\frac{1}{\sqrt{n\log n}}\right)^{1} \text{ per } S\text{-}D \text{ pair.} \tag{1}$$

A throughput $t > 0$ is feasible if every node in a network can send t bits-per-second.

(ii) Delay: the delay is the time of a packet to reach the destination after leaving source in a network.

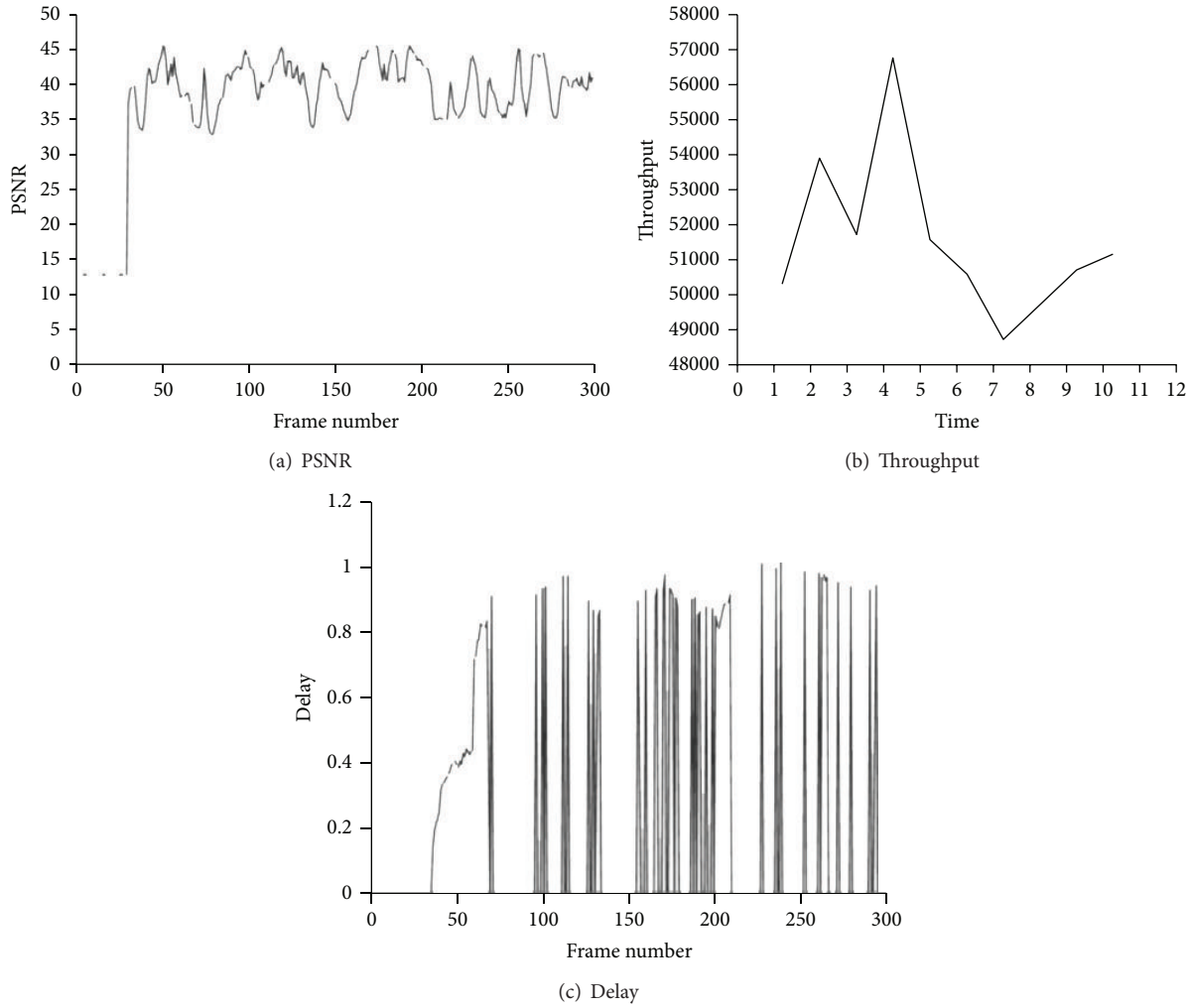
(iii) Peak signal noise ratio (PSNR): PSNR is used to measure the error between transmitted multimedia data and the original data. The equation below defines the PSNR between component Y of source S and destination D:

$$\mathrm{PSNR}\,(n) = 20\log_{10}\left\{\frac{M_{\mathrm{peak}}}{\sqrt{\left(1/N_{\mathrm{col}}N_{\mathrm{row}}\right)\sum_{i=0}^{N_{\mathrm{col}}}\sum_{j=0}^{N_{\mathrm{row}}}\left[Y_S\left(n,i,j\right)-Y_D\left(n,i,j\right)\right]^2}}\right\}, \tag{2}$$

where $M_{\mathrm{peak}} = 2^m - 1$ and m: number of bits per pixel.

In the first scenario, we measure the delay, PSNR, and throughput without using the proposed framework. In the second scenario, we perform the same analysis by implementing the proposed framework for detection of malicious node and data. In these simulations, we assume that each sensor can only directly communicate with its neighbor sensors. Sensor node 1 wants to send its secure message to Sensor node 2. The secure message will be communicated through the proposed framework and verified for malicious node and data identification. To give a detailed experiment analysis, we further analyze and compare the throughput, delay, and PSNR in the WSNs.

4.1. Study Scenario I: Performance Analysis in Ideal State. In this study, we analyze the performance in ideal state (i.e.,



(a) PSNR

(b) Throughput

(c) Delay

FIGURE 5: Analysis results in ideal state.

no proposed framework to detect malicious data and node), which gives us results for comparative performance analysis when we apply our proposed framework to determine the redundant messages, malicious data, and nodes in WSNs. Here, we have highlighted three sensor nodes: S1, S2, and S3. Sensor nodes S2 and S3 want to share secure data with sensor node S1, where S2 is malicious, that is, sending malicious data to S1 in order to degrade the performance of WSNs as shown in Figure 4. As mentioned, system is not able to validate the malicious activities and data due to lack of secure wireless communication framework. The system assumes that all network nodes are fair. Analysis results are given in Figure 5; the computed delay in this communication is higher as shown in Figure 5(b) and the throughput is lower as shown in Figure 5(c) because S2 is malicious and sends malicious data to S1. Figure 5(a) shows reconstruction peak signal-to-noise ratio (PSNR) for all frames in the network.

4.2. Study Scenario II: Performance Analysis with Proposed Framework. In this study, we simulate the same scenario as we did in study I with the proposed secure wireless communication framework. As mentioned earlier, Sensor

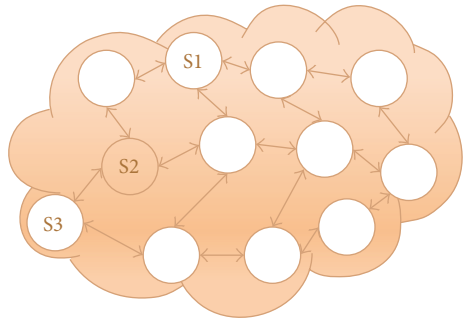
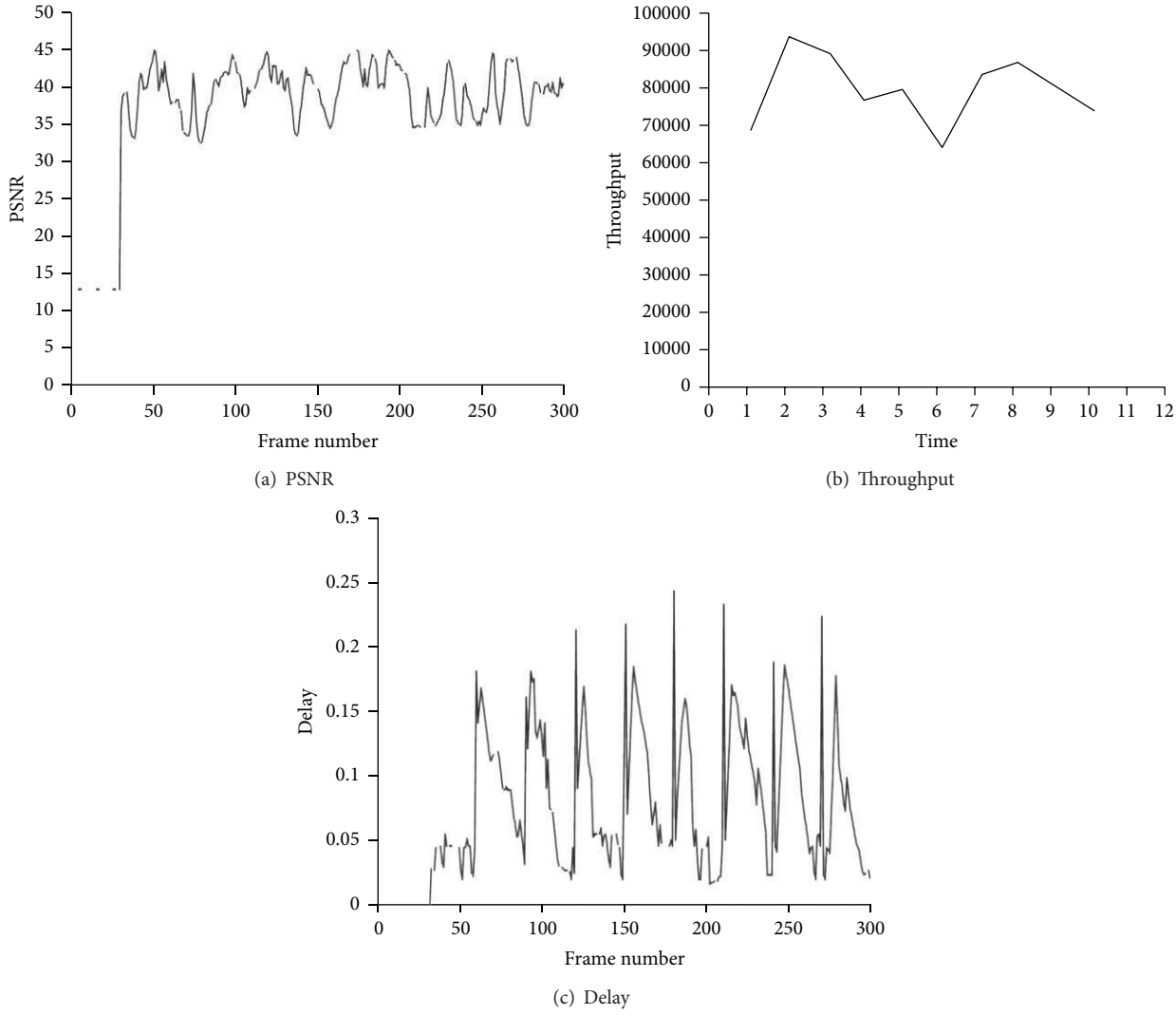


FIGURE 6: Sensors nodes network with secure wireless communication framework.

nodes S2 and S3 want to share secure data with Sensor node S1, where S2 is a malicious and sends malicious data to S1 in order to degrade the performance of WSNs as shown in Figure 6 but here the message is communicated through secure framework to check message redundancy, determine message priority, and detect and verify malicious node and data.



(a) PSNR

(b) Throughput

(c) Delay

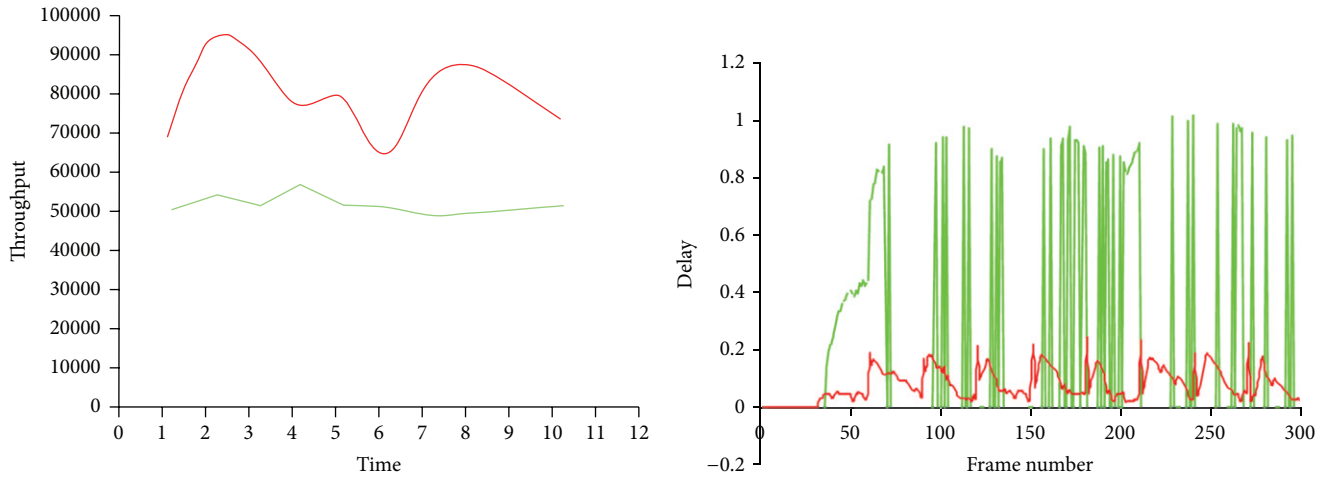
Figure 7: Analysis results with secure wireless communication framework.

The delay, PSNR, and throughput have been computed using the proposed secure wireless communication framework as shown in Figure 7. Experiment results show that sensor network performance is consistent and acceptable. It is stable and suitable to prevent the network degradation with proper implementation. It detects malicious data during message transmission from neighbours. Experiment shows that PSNR analysis results are the same in both simulations as shown in Figures 5(a) and 7(a). Figures 5(b) and 5(c) show that computed throughput is higher and delay is lower, respectively, because framework detects the malicious data without degrading network performance.

4.3. Comparison. In the following, we present and discuss the simulation comparison results. We performed the simulation for both scenariosL: in the first scenario the framework was in ideal state and in the second scenario the framework was present for malicious node and data detection. Simulation parameter values are given in Table 1. In both runs of the simulation, we set Sensor node S2 as a malicious node that is sending malicious data in order to degrade the performance of WSNs. Right before the beginning of malicious activities, all statistics are readjusted to zero. In each scenario, we measure the delay, throughput, and PSNR to determine the level of security and performance of the proposed framework. Comparison graphs of delay and throughput measurements are given in Figure 8. It is clear that the use of the proposed secure wireless communication framework increases the throughput and decreases the delay for the detection of malicious nodes and data. However, it was reversed when we tested the same without the proposed framework. Experiment results indicate that the performance is acceptable for secure wireless communication. Thus, the proposed framework is suitable and practical for real-time use.

5. Conclusions

With large-scale and rapid development in wireless sensor networks (WSNs), there is great demand to adopt security



(a) Throughput (b) Delay

Figure 8: Comparison results.

mechanisms for secure wireless communication. WSNs have many fields of applications that are playing an essential role in increasing productivity and reducing cost. However malicious attackers can access the transmission, threaten users, and alter or misuse communication illegally due to restricted and constrained nature of sensors with potentially dynamic behavior of WSNs. Therefore security becomes serious issue and concern to prevent illegal use or access and protect communication from various attacks. We proposed a framework for secure wireless communication in WSNs which consists of four modules, that is, redundancy checker, message prioritization mechanism, malicious node verification and malicious data verification. We present and discuss the simulation results of security and performance analysis for comparison and evaluate the proposed framework. Experiment results indicate that the performance of the framework is acceptable for malicious node and data detection in WSNs and suitable for real-time use.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] A. Alemdar and M. Ibnkahla, "Wireless sensor networks: applications and challenges," in *Proceedings of the 9th International Symposium on Signal Processing and its Applications (ISSPA '07)*, pp. 1–6, IEEE Computer Society, Washington, DC, USA, February 2007.

[4] T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Proceedings of the 20th IEEE International Symposium on Intelligent Control—Mediterranean Conference on Control and Automation (ISIC '05)*, pp. 719–724, IEEE Computer Society, Washington, DC, USA, June 2005.

[5] D. Liu and P. Ning, *Security for Wireless Sensor Networks*, Advances in Information Security Series, Springer, 2006.

[6] J. López and J. Zhou, *Wireless Sensor Network Security*, Cryptology and Information Security Series, IOS Press, 2008.

[7] K. Ren and W. Lou, *Communication Security in Wireless Sensor Network*, VDM Verlag Dr. Müller, 2008.

[8] D. Liu, P. Ning, S. Zhu, and S. Jajodia, "Practical broadcast authentication in sensor networks," in *Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '05)*, pp. 118–129, July 2005.

[9] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 11, pp. 4136–4144, 2007.

[10] A. Hac, *Wireless Sensor Network Designs*, John Wiley & Sons, New York, NY, USA, 2003.

[11] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05)*, pp. 11–21, Alexandria, VA, USA, November 2005.

[12] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04)*, pp. 29–37, Philadelphia, Pa, USA, October 2004.

[13] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS '06)*, Los Angeles, Calif, USA, September 2006.

[14] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, 2006.

[15] K. Nahrstedt, J. Dittmann, and P. Wohlmacher, "Approaches to multimedia and security," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '00)*, pp. 1275–1278, New York, NY, USA, August 2000.

[16] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[17] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[18] A. Rahim, Z. Shafi Khan, F. T. Bin Muhaya, M. Sher, and T. H. Kim, "Sensor based framework for secure multimedia communication in VANET," *Sensors*, vol. 10, no. 11, pp. 10146–10154, 2010.

[19] F. Bai, N. Sadagopan, and A. Helmy, "The important framework for analyzing the impact of mobility on performance of routing protocols for Ad hoc Networks," *Ad Hoc Networks*, vol. 1, no. 4, pp. 383–403, 2003.

[20] Network Simulator, "NS-2," 2010, http://www.isi.edu/nsnam/ns/.

[21] C.-H. Ke, C.-K. Shieh, W.-S. Hwang, and A. Ziviani, "An evaluation framework for more realistic simulations of MPEG video transmission," *Journal of Information Science and Engineering*, vol. 24, no. 2, pp. 425–440, 2008.

[22] Cygwin, 2010, http://www.cygwin.com/.