



An energy-efficient lightweight security protocol for optimal resource provenance in wireless sensor networks

Sujesh LAL^{1,*} , Joe PRATHAP² 

¹Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

²Department of Information Technology, RMD Engineering College, Anna University, Chennai, India

Received: 02.03.2020

Accepted/Published Online: 19.06.2020

Final Version: 30.11.2020

Abstract: Security of resource sharing and provenance is a major concern in wireless sensor networks (WSNs), where the intruders can easily inject malicious intermediate nodes for various personal gains. This selective forwarding attack may reduce the flow of resource sharing and throughput in the network. Most of the existing techniques are complex and do not provide sufficient security to sensor nodes with low energy. This paper proposes an energy-efficient and lightweight security protocol for optimal resource provenance in multihop WSNs and the Internet of things (IoT) network. The sharing of the resources between the sensor nodes indicates the strength of the mutual cooperation between the nodes, which will act as a link to generate a cooperative correlating coefficient in the proposed security protocol. The cooperative correlating coefficient is computed and matched at the source and destination sensor node, which is broadcast to all the connecting intermediate sensor nodes. A higher value of the cooperative correlating coefficient indicates stronger and secure resource sharing between the sensor nodes with optimal resource provenance, and the lower value indicates the possibility of the presence of adversarial sensor nodes between the hops. We calculate the energy dissipated for the sensor nodes and the complete sensor network. The real-time cooperative correlating coefficient values are derived from the cooperation of two USRPs. The simulation for the detection of adversarial sensor node and resource provenance is done using MATLAB. The experimental result demonstrates secure resource provenance sharing in a sensor network with high energy efficiency compared to the existing techniques.

Key words: Energy efficiency, Internet of things, provenance, resource sharing, security and privacy, wireless sensor network

1. Introduction

Wireless sensor networks (WSNs) emerged as one of the most powerful communication technologies of the 21st century. WSNs and IoT have become an indispensable part of life with numerous connected devices at home and work managing many vital tasks. Most of these connected devices like medical sensors and vehicular sensors are designed for seamless interaction with good storage and computational capabilities [1–4]. IoT and WSNs are currently deployed in applications in healthcare, home automation, military, and transportation [5–9]. The major challenge with this rapid development and expansion of WSNs and IoT is in ensuring security and privacy. As hundreds of sensors are connected to the network from various locations, it is vital to secure the sensitive data transferred through the network as well as the data stored in the devices [10–13]. Unauthorized access to the network and the devices can lead to serious consequences, especially in many healthcare and military applications [14, 15]. In these networks, the data is collected by the sensor node and sent to the centralized

*Correspondence: sujeshlal@fisat.ac.in

server for processing and monitoring. Here, the data has to pass through a number of intermediate nodes in the network located at various locations. These nodes collect, process, and make decision on resource sharing in the network for efficient routing. All the nodes collect and pass provenance data for authentication in the network.

Although many mechanisms are proposed to ensure secrecy of data in WSN, the security of provenance is currently a major area of concern where the intruders can easily inject malicious intermediate nodes for various personal gains [16, 17]. This selective forwarding attack may reduce the flow of resource sharing and throughput. Most of the existing techniques are complex and do not provide sufficient security to sensor nodes with low energy. A detailed investigation of secure provenance schemes and its associated security issues have been presented in [17]. In [18], authors discuss a light-weight protocol for data provenance in IoT that uses physical unclonable functions (PUFs). Data provenance schemes based on block chains have also been proposed recently [19]. Various issues and challenges with data provenance in WSNs and IoT are also discussed in [20, 21].

In this paper, we propose a lightweight security protocol for optimal resource provenance in multihop WSNs and IoT networks. The sharing of the resources between the sensor nodes indicates the strength of the mutual cooperation between the nodes, which will act as a link to generate a cooperative correlating coefficient (CCC) in the proposed security protocol. The CCC is computed and matched at the source and destination sensor node, which is broadcast to all the connecting intermediate sensor nodes. A higher value of CCC indicates stronger and secure resource sharing between the sensor nodes with optimal resource provenance, and the lower value indicates the possibility of the presence of adversarial sensor nodes between the hops. We calculate the energy dissipated for the sensor nodes and the complete sensor network. The real-time CCC values are derived from the cooperation of two USRP, and the simulation for the detection of adversarial sensor node and resource provenance is done using MATLAB 2018a. Results obtained highlight the better performance of the proposed approach compared to previous techniques in secure resource provenance. The remaining section is organized as follows. Section 2 discusses related works in the current research area. Section 3 discusses the proposed work in detail. The system model used is discussed, along with theoretical analysis. Also, the algorithms used for secure resource provenance is presented. The results and discussion are presented in Section 4, and the paper concludes in Section 5. The list of frequently used notations is given in Table 1 and the list of abbreviations used in the paper is given in Table 2.

Table 1. Frequently used notations.

| Notation | Definition |
|----------------|--|
| P_{rec} | Received power by sensor node |
| P_{tx} | Transmitted power by sensor node |
| G_{at} | Gain of transmitting antenna |
| G_{ar} | Gain of receiving antenna |
| L_{pth} | Path loss |
| D | Distance between the sensor nodes |
| λ | Wave length |
| $P_{rec(max)}$ | Max value of the received power |
| $P_{rec(min)}$ | Min value of the received power |
| S_{KN1} | Secret key for SN1 |
| R_i, R_j | Cooperation ratio for the i^{th} sensor node |

Table 2. List of abbreviations.

| Abbreviation | Description |
|--------------|---------------------------------------|
| UASN | Underwater acoustic sensor networks |
| USRP | Universal software radio peripheral |
| IoT | Internet of things |
| PUF | Physical unclonable functions |
| PI | Phaser information |
| ToA | Time of arrival |
| TP | Transmit power |
| RP | Receive power |
| EVM | Error vector magnitude |
| TRSS | Transmit and received signal strength |
| SN1 | Sensor node 1 |

2. Related work

This section discusses some of the recent work on secure resource provenance in WSNs and IoT. In [17], a detailed study and analysis of existing secure provenance schemes are presented. The study discusses the use of provenance in WSNs and IoT, and also the importance of securing provenance. A detailed classification of the existing secure provenance methods is presented, and the issues related to each of the techniques are highlighted and discussed. A light-weight protocol for secure provenance in IoT using physical unclonable functions is discussed in [18]. The technique highlights the need for proper authentication of data coming from numerous connected low-cost sensors. Block chain is currently used to provide high security in data transmission in various networks. A method to secure provenance in a cloud environment is discussed in [19]. The major advantage with the block chain-based methods is that it can provide tamper-proof records and enable the transparency of data accountability in the cloud network. The importance of providing secure data provenance throughout the whole life-cycle of the IoT devices connected in the network is discussed in [20]. In [21], various design requirements of data provenance in IoT are analyzed, and the existing issues are highlighted. A method for ensuring security with provenance data using Bloom filter is discussed in [22]. This technique was designed mainly for low-cost sensors with limited storage and computational capabilities. An interesting technique for secure data provenance for data-intensive applications is proposed in [23]. The authors discussed the importance of designing effective provenance management systems in these types of networks. A secure provenance architecture with low overhead is proposed in [24]. This system is designed to react automatically on detecting low trust between the nodes in the network. In [25], a technique for secure provenance in IoT networks is discussed. Although many pieces of work have discussed secure provenance transmission and resource sharing, most of them are complex and do not consider the energy level of various devices in the network. As most of the connected devices include low-cost sensors, it is very vital to limit the energy usage and extend the lifetime of devices in the network. To overcome these challenges, we propose an energy efficient and lightweight security protocol for optimal resource provenance in wireless sensor networks. The next section discusses the proposed technique in detail.

3. Proposed system

In this section, we present and discuss the proposed system for optimal resource provenance in multi-hop wireless sensor networks. Initially, the designed system model is presented and discussed in detail. The theoretical analysis of the proposed work is then discussed along with the algorithms for the generating and encoding of CCC and for the detection of adversarial sensor nodes in multihop wireless sensor networks.

3.1. System model

Figure 1 presents the system model of the proposed security protocol. When two sensor nodes communicate, there are various parameters like phaser information (PI), time of arrival (ToA), transmit power (TP), receive power (RP), throughput, and error vector magnitude (EVM) that are considered for generating the cooperative correlating coefficient (CCC) in the WSN network. The transmit and received signal strength (TRSS) has a direct relation with the CCC. The value of TRSS is recorded in real-time using USRP. Depending on the transmit and receive power, the value of TRSS can be varied to maintain the optimal power at the nodes. For performing the simulation and experiment, the following four scenarios are considered: the sensor network having no adversarial nodes, the sensor network having adversarial nodes between sensor node SN1 and SN2, the resources shared and tampered at the sensor node, and the sensor nodes replaced by the adversarial node.

The proposed solution validates the security in all the mentioned cases by consuming very little power. The real-time values for the USRP nodes deployed in a sensor network is then calculated.

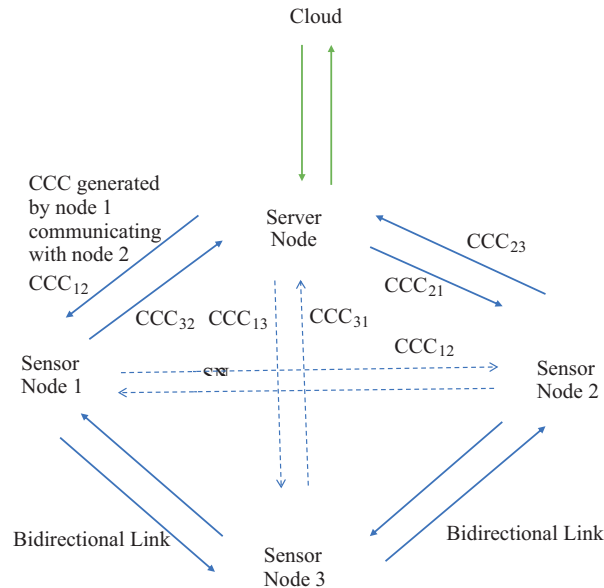


Figure 1. System model.

3.2. Theoretical analysis

3.2.1. Detection of adversarial node

Each sensor node in WSN and IoT networks records the CCC value every 10 s. The CCC values are in dBm range. The power of the transmitted and received signal is calculated by using the Friis transmission equation. Here P_{rec} is the received power by the sensor node, P_{tx} is the transmitted power by the sensor node, and G_{at} , G_{ar} are the gain of the transmitted and receiving antenna respectively and L_{Pth} is the path loss during transmission. The path loss is large, and the received power by sensor node is small; hence, CCC is also small. The path loss for transmission is given by $L_{Pth} = \left(\frac{4\pi D}{\lambda}\right)^2$. Here ‘D’ is the distance between the sensor nodes and λ is the wavelength. The value of λ is 400 nm, and the operating frequency of USRP is 2.4 GHz. The gain value is chosen as 60 to make the measured value positive. The quantization of CCC is done using the word length of 16 bit and having 2^{16} levels L_B . The magnitude of measuring and dividing the optimal CCC in Min and Max values and mapping it into ‘Z’ fragment. The magnitude has height ‘h’. This is represented as $h = \frac{P_{rec(max)} - P_{rec(min)}}{Z}$. The $P_{rec(max)}$ and $P_{rec(min)}$ are the max and min value of the received power. Then, the fragment centre is assigned the value from 0 to Z-1. The signal of the sample falling in the fragment is round off to the centre value. Then, each fragment is crippled a word length of 16 bit ‘Ncc’. These 16 bit is the CCC value. This CCC value is encoded with a 16-bit secret key. The secret key is S_{KN1} for SN1, S_{KN2} for SN2, and S_{KN3} for SN3. The encoded CCC is given by:

$$EN_{CCC[1 \rightarrow N]} = N_{CCC[1 \rightarrow N]} \oplus E_{CCC} S_{KN} \tag{1}$$

Each sensor node maintains its own secret key and CCC without sharing it with other sensor nodes. The server node is assumed to be highly secure and resource sharing is done only after authentications.

3.2.2. Transmit/receive signal strength for SN and CCC analysis

The transmit and receive signal strength for the sensor node using CCC is presented in this section. The transmit power is limited, and it has to be distributed by considering optimal CCC as the target represented as CCC_i and CCC_j for the transmit node and the receiving node in the given architecture. The cooperation and provenance of the transmit/receive nodes are utilized to address the mentioned problem. To satisfy the optimal CCC target, the following condition for transmission power signal strength of i^{th} and j^{th} sensor nodes have to be satisfied,

$$\begin{aligned} TRSS_i &= v_i^2 [f] \geq (\sigma_w^2 / SN_{ij}^2) CCC_i \\ TRSS_j &= v_j^2 [f] \geq (\sigma_w^2 / SN_{ij}^2) CCC_j \end{aligned} \quad (2)$$

Initially we start with the power analysis of the transmit and receive nodes. Here the transmission power signal strength for sensor node source 'i' in the occupied frequency spectrum 'f' is given as TRSS_i [f]. The TRSS power allocation at the i^{th} sensor node is given by,

$$TRSS_i[f_1] = \sum v_i^2[f_1] \quad (3)$$

We then analyze the power allocation for different frequency slots. The TRSS power allocation at frequency slot $f_2 - f_1$ is given by,

$$TRSS_i[f_2 - f_1] = \sum [f_2 - f_1] (SN_{ij}^2 v_j^2 [f_2 - f_1] + \sigma_n^2) \quad (4)$$

The TRSS power allocation at source j for frequency slot $(1 - f_2)$ is given by:

$$TRSS[(1 - f_2)] = \sum a_j^2 [(1 - f_2)] \quad (5)$$

The TRSS power allocation at source j for frequency slot $(1 - f_1)$ is given by:

$$TRSS_j[(1 - f_1)] = \sum [(1 - f_1)] (SN_{ji}^2 v_j^2 [(1 - f_1)] + \sigma_w^2) v_j^2 \quad (6)$$

The total TRSS transmission power for sensor node source i is represented as:

$$TRSS_i = \sum TRSS_i[f_1] + TRSS_i[f_2 - f_1] \quad (7)$$

The optimal TRSS transmit power for sensor node source j is given as:

$$TRSS_j = \sum TRSS_j[f_1 - f_2] + TRSS_j[1 - f_1] \quad (8)$$

The net TRSS transmit power of all sensor nodes are represented by:

$$TRSS_{total} = TRSS_i + TRSS_j \quad (9)$$

Now we aim at deriving the optimal criteria for "CCC" at all the sensor transmitting nodes in the system. For this we can analyze the above equations and results. The CCC for the i^{th} transmitter is represented as the

ratio of signal strength allocated at a given spectrum for the j^{th} source's collaborative retransmission to the signal strength of the original transmission of sensor node source $j (i \neq j)$. From eqs. 4 and 6, the cooperation ratio for the i^{th} sensor node is computed as:

$$[R_i] = (TRSS_i[f_2 - f_1]) / (TRSS_j[1 - f_2]) = (a_i^2[f_2 - f_1](C_i j^2 v_j^2[1 - f_2] + \sigma_n^2)) / (v_j^2[1 - f_2]) \quad (10)$$

for $0 \leq R_i < \infty$ and $j \neq i$.

$$[R_j] = (TRSS_j[1 - f_1]) / (TRSS_i[f_1]) = (a_i^2[1 - f_1](S N_i j^2 v_i^2[f_1] + \sigma_w^2)) / (v_j^2[f_1]) \quad (11)$$

for $i, j \in \{1, 2, 3, 4, 5\}$ and $0 \leq R_j < \infty$ and $j \neq i$. The noncooperative condition points to: $[R_i] = [R_j] = 0$

3.2.3. Signal strength sharing at received SN and CCC analysis

The CCC of sensor node at the receiving side is to be calculated on the presumed condition that the receiving sensor node optimally combine $\{rc_{ij}, rsc_{ij}\}$ to CCC. The mutual and random noises are considered exclusively from the information of messages. Thus, it is concluded that the maximum CCC combining at the receiving nodes optimize the CCC of rc_{ij} and rsc_{ij} . The optimal CCC coefficients can be represented as:

$$(\Gamma_i[f_2 - f_1]) / (\Gamma_i[f_1]) = (C_i j v_j [f_2 - f_1] \sigma_w^2) / ((\sigma_w^2 + C_i j^2 v_j^2 [f_2 - f_1] \sigma_n^2)) \quad (12)$$

$$(\Gamma_i[1 - f_2]) / (\Gamma_i[1 - f_1]) = (C_i j v_i [1 - f_2] \sigma_w^2) / ((\sigma_w^2 + C_i j^2 v_i^2 [1 - f_2] \sigma_n^2)) \quad (13)$$

The CCCs calculated with optimal compounding at the receiving sensor node can be represented as:

$$[CCC_j = U_{(f_1)}^1 \cdot (C_i j^2 v_j^2 [1 - f_1]) / (\sigma_w^2) + (C_i j^2 v_i^2 [1 - f_1] C_i j^2 v_j^2 [1 - f_1]) / (\sigma_w^2 + C_i j^2 v_i^2 [1 - f_2] \sigma_n^2)] \quad (14)$$

We now need to obtain the CCC of each transmitting sensor node in the network. It is obtained by substituting eqs. 10 and 11 into eqs. 14 and 15 and given by:

$$CCC_i = \int_{f_1}^{f_2} \frac{C_{ij}^2 P_i [f_2 - f_1]}{\sigma_w^2} + \frac{R_j P_i^2 [f_2 - f_1] C_{ij}^4}{\sigma_w^2 (C_{ij}^2 P_i [f_1] + \sigma_n^2) + R_i P_i [f_1] C_{ij}^2 \sigma_n^2} \quad (15)$$

$$CCC_j = \int_1^{f_2} \frac{C_{ij}^2 P_i [1 - f_1]}{\sigma_w^2} + \frac{R_j P_i^2 [1 - f_1] C_{ij}^4}{\sigma_w^2 (C_{ij}^2 P_i [f_1] + \sigma_n^2) + R_i P_i [f_1] C_{ij}^2 \sigma_n^2} \quad (16)$$

The inference of CCC for i^{th} and j^{th} sensor node CCC_i, CCC_j and the cooperative ratios R_i, R_j between them allow us to completely analyze the optimal transmission power at the sensor nodes for all different SN nodes and the optimal collaboration among them.

3.2.4. Adversarial node replaces sensor node and sends the data to the server node:

Here, S_{KN1} , S_{KN2} , and S_{KN3} are the secret keys shared with the server. The server node decodes all the resources shared from different sensor nodes using the secret key associated with the representative sensor node.

$$N_{CCC[1 \rightarrow N]} = EN_{CCC[1 \rightarrow N]} \oplus S_{KN} \quad (17)$$

The decoded value of CCC is converted to decimal value in dBm and the Pearson correlation coefficient is performed to find optimal CCC value. If the value lies between 0.7 and 1, the CCC has high correlation and if it is between 0 and 0.2 it has low correlation.

$$\zeta_{R_1 R_2} = \frac{CON(R_1 R_2)}{\sigma_{R_1} \sigma_{R_2}} \quad (18)$$

The correlation coefficient 'C' is calculated as:

$$C = \frac{\prod_{i=1}^n (R_1 - \hat{R}_1) \prod_{i=1}^n (R_2 - \hat{R}_2)}{\sqrt{\prod_{i=1}^n (R_1 - \hat{R}_1)^2} \sqrt{\prod_{i=1}^n (R_2 - \hat{R}_2)^2}} \quad (19)$$

where R_1 and R_2 are the CCC value of the resource shared at sensor node SN1 and SN2 and \hat{R}_1 and \hat{R}_2 are the mean for the 'N' segment of resources. The correlation coefficient will have three values, where 1 is for perfect CCC, 0 is for no CCC and -1 for inverse CCC. The server node correlates the CCC value of the neighboring sensor node. The absence of adversarial node in the sensor network indicates the high CCC value. The intrusion of adversarial node between SN1 and SN2 interrupts the resource sharing and the CCC value received at SN1 and SN2 will be different. The value of CCC will change depending on the level of intrusion. The server node does the decoding with the secret key already shared by the sensor node.

Algorithm for the generating and encoding of CCC

1. Initialize $j = 1 \rightarrow n, k = 1 +$ number of nodes.
2. Initialize the sensor node and bidirectional transfer of resources
3. Received power P_{rec} from neighbor is $P_{recCurrent}[j] \leftarrow P_{recCurrent}[j] + G$
4. Quantize the word length $P_{recCurrent}[j]$.
5. $CCC[j] \leftarrow$ binary code assigned to quantized $P_{recCurrent}[j]$.
6. $EN_{CCC}[j] \leftarrow XOR(N_{CCC}[j], \zeta_{KN}[k])$.
7. EN_{CCC} copy at corresponding sensor node sent to server node.

Algorithm for detection of adversarial sensor node in the IoMT

1. $EN_{CCC}[j] \leftarrow XOR(EN_{CCC}[j], \zeta_{KN1}[j])$.
2. $P_{recCurrent}[j] \leftarrow Bin - DecConv(N_{CCC}[j])$

3. $N_{CCC} [j] \leftarrow XOR (EN_{CCC} [j], \zeta_{KN2} [j])$
4. $P_{recurrent} [k] \leftarrow Bin - DecConv (N_{CCC} [k])$.
5. $\zeta (P_{recurrent} [j], P_{recurrent} [k])$
6. if $[0.8 < \zeta \leq 1]$, then
7. return adversarial node absent
8. else if $\zeta = -1$ to 0.8 , then
9. return adversarial node present
10. else return $[P_{rec}$ values are not shared properly
11. end if.

For the resource provenance, the header information is analyzed to reach the origin node for resources. The header details are present in the server node as each sensor node copies the CCC at the server node. The resource shared to node 2 from sensor node1 routed through sensor node 3, the CCC of the headers are compared in the server in the sequence it is received. The last headers received from the sensor node are compared, and it converges as origin node. The sensor node forms the header information using CCC and forwards it to the neighboring sensor node. The neighboring sensor node receives and forwards by attaching the header information using its CCC. The transmission converges to the end node where the end node adds its own header and passes it to the server node. The server node has the information of the header attached by different sensor nodes and its neighbor. To verify the origin node, server nodes decode the header information with secret key and correlative CCC with the CCC already received by different nodes. The matching of the CCC enables the same process repeated to the adjacent node, this continues till all the header information of sensor nodes is exhausted, and high value for CCC is achieved. If a mismatch occurs in the CCC value, the node corresponding to the sensor node for the CCC value will be the node where information is trans/received. This process can help us in finding the links where exactly the information has been forged. Thus, secure and optimal resource provenance is achieved.

4. Results and discussion

The proposed secure resource provenance sharing method is applied to the WSN and IoT network through simulation in MATLAB 2018a. The results of the simulation are presented and discussed in this section. Figure 2 presents the transmit-receive amplitude of the signal and the transmit-receive power of the signal with varying time when cooperative correlating coefficient (CCC) is not used. Here we can observe that the amplitude and power of the signal for transmitting and receiving nodes is constant with varying time in normal scenarios.

Figure 3 presents the transmit-receive amplitude of the signal and the power of the signal with varying time when CCC is used. It can be observed that the amplitude of the signal is maximum when the power transmitted between the nodes is high. Here the sharing of the resources between the sensor nodes indicates the strength of the mutual cooperation between the nodes, which will act as a link to generate the CCC.

Figure 4 presents the cooperative correlating coefficient and the transmit-receive power with varying time. It is observed that, as the transmit-receive power is high, the cooperative correlating coefficient is also high. The CCC is computed and matched at the source and destination sensor node, which is broadcasted to all the

connecting intermediate sensor nodes. Higher value of cooperative correlating coefficient indicates stronger and secure resource sharing between the sensor nodes with optimal resource provenance. This scenario is without the presence of any adversarial sensor node in the network. In Figure 5, we can observe that, in presence of an adversarial node in the network, the amplitude and power do not have uniform variations; hence, the cooperative correlating coefficient value will be less. Thus, using the proposed approach, we can attain optimal resource provenance sharing between the nodes and also efficiently detect malicious nodes in the network.

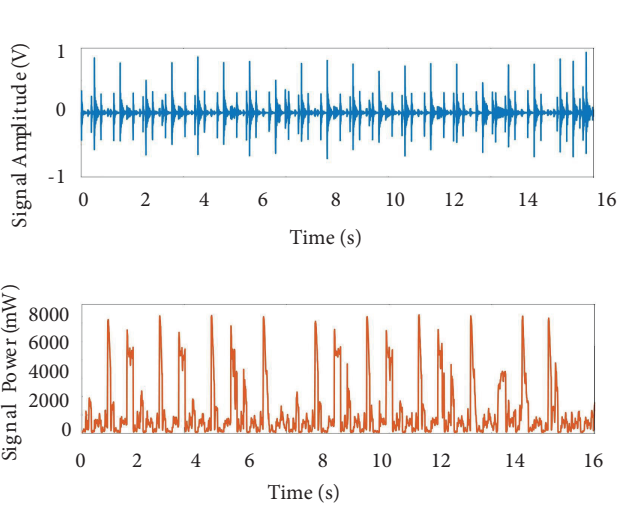


Figure 2. Variation in Transmit-Receive amplitude and power of the signal with time when CCC is not used

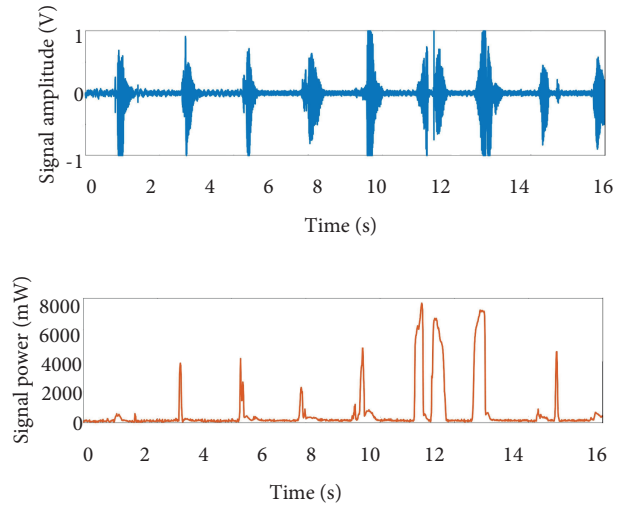


Figure 3. Variation in Transmit-Receive amplitude and power of the signal with time when CCC is used

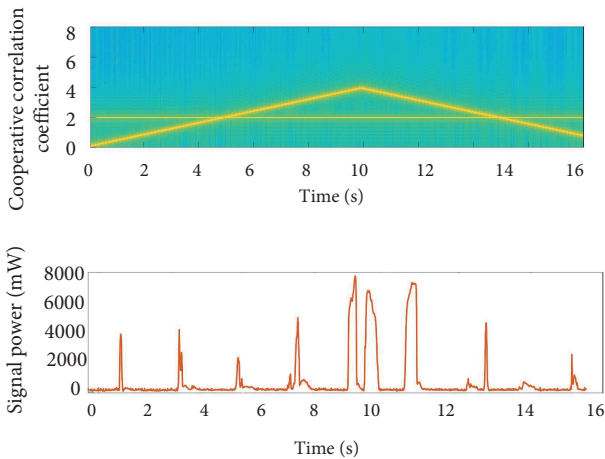


Figure 4. Variation in Cooperative Correlating Coefficient and power with time

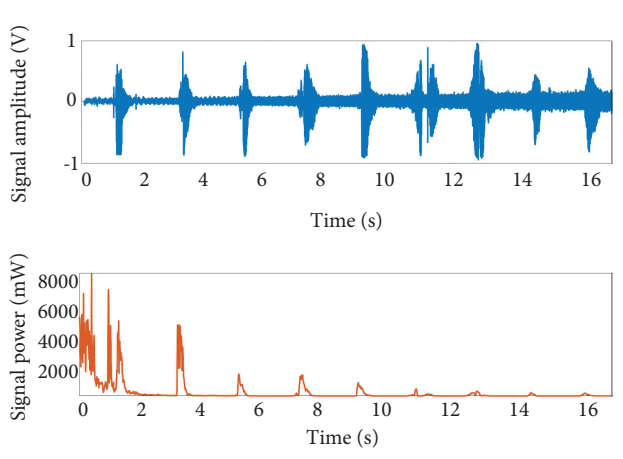


Figure 5. Variation in transmit-receive amplitude and power of the signal with time when adversarial node is present.

5. Conclusion

In WSN and IoT applications, security of resource sharing and provenance is a major area of concern where the intruders can easily inject malicious intermediate nodes for various personal gains. In this paper, we proposed a lightweight security protocol for optimal resource provenance in multihop WSN. The system model and theoretical analysis were presented and discussed in detail. The newly proposed cooperative correlating coefficient (CCC) value was used to determine the presence of adversarial sensor nodes between the hops in the network. The real-time CCC values are derived from the cooperation of two USRP and the simulation for the detection of adversarial sensor node and resource provenance was done using MATLAB. The experimental result demonstrated secure resource provenance sharing in sensor network with high energy efficiency compared to the existing techniques.

References

- [1] Ayaz M, Ammad-uddin M, Baig I, Aggoune EM. Wireless sensor's civil applications, prototypes, and future integration possibilities: a review. *IEEE Sensors Journal* 2018; 18 (1): 4-30. doi: 10.1109/JSEN.2017.2766364
- [2] Sevin A, Bayılmış C, Ertürk İ, Ekiz H, Karaca A. Design and implementation of a man-overboard emergency discovery system based on wireless sensor networks. *Turkish Journal of Electrical Engineering and Computer Sciences* 2016; 24(3): 762-773. doi: 10.3906/elk-1308-154
- [3] Liu Y, Lam KY, Han S, Chen Q. Mobile data gathering and energy harvesting in rechargeable wireless sensor networks. *Information Sciences* 2019; 482: 189-209. doi: 10.1016/j.ins.2019.01.014
- [4] Farsi M, Elhosseini MA, Badawy M, Ali HA, Eldin HZ. Deployment techniques in wireless sensor networks, coverage and connectivity: a survey. *IEEE Access* 2019; 7: 28940-28954. doi: 10.1109/ACCESS.2019.2902072
- [5] Ball G, Qela B, Wesolkowski S. A review of the use of computational intelligence in the design of military surveillance networks. *Recent Advances in Computational Intelligence in Defense and Security* 2016; 621: 663-693. doi: 10.1007/978-3-319-26450-9.
- [6] Menon VG, Jacob J, Joseph S, Almagrabi AO. SDN powered humanoid with edge computing for assisting paralyzed patients. *IEEE Internet of Things Journal* 2019; 1: 1-20. doi: 10.1109/JIOT.2019.2963288
- [7] Gökbayrak A, Kılıvan S, Akın S, Çelebi A, Urhan O. Wireless sensor network-based extension to KNX home automation system. *Turkish Journal of Electrical Engineering and Computer Sciences* 2016; 24(5): 3652-3663. doi: 10.3906/elk-1407-47
- [8] Vinoj G, Jacob S, Menon V, Rajesh S, Khosravi M. Brain-controlled adaptive lower limb exoskeleton for rehabilitation of post-stroke paralyzed. *IEEE Access* 2019; 7: 132628-132648. doi: 10.1109/ACCESS.2019.2921375
- [9] Yaacoub J, Noura M, Noura HN, Salman O, Yaacoub E et al. Securing internet of medical things systems: limitations, issues and recommendations. *Future Generation Computer Systems* 2020; 105: 581-606. doi: 10.1016/j.future.2019.12.028
- [10] Tomić I, McCann JA. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal* 2017; 4(6): 1910-1923. doi: 10.1109/JIOT.2017.2749883
- [11] Pritchard SW, Hancke GP, Abu-Mahfouz AM. Security in software-defined wireless sensor networks: threats, challenges and potential solutions. In: *Proceedings of IEEE 15th International Conference on Industrial Informatics (INDIN)*; Emden, Germany; 2017. pp. 168-173. doi: 10.1109/INDIN.2017.8104765
- [12] Andrea I, Chrysostomou C, Hadjichristofi G. Internet of things: security vulnerabilities and challenges. In: *Proceedings of the IEEE Symposium on Computers and Communication (ISCC)*; Larnaca, Cyprus; 2015. pp. 180-187. doi: 10.1109/ISCC.2015.7405513

- [13] Ahanger TA, Aljumah A. Internet of things: a comprehensive study of security issues and defense mechanisms. *IEEE Access* 2019; 7: 11020-11028. doi: 10.1109/ACCESS.2018.2876939
- [14] Sun Y, Lo FP, Lo B. Security and privacy for the internet of medical things enabled healthcare systems: a survey. *IEEE Access* 2019; 7: 183339-183355. doi: 10.1109/ACCESS.2019.2960617
- [15] Rajesh S, Paul V, Menon VG, Jacob S, Vinod P. Secure brain to brain communication with edge computing for assisting post-stroke paralyzed patients. *IEEE Internet of Things Journal* 2019; 1: 1-20. doi: 10.1109/JIOT.2019.2951405
- [16] Alkhalil A, Ramadan RA. IoT data provenance implementation challenges. *Procedia Computer Science* 2017; 109: 1134-1139. doi: 10.1016/j.procs.2017.05.436.
- [17] Zafar F, Khan A, Suhail S, Ahmed I, Hameed K et al. Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. *Journal of Network and Computer Applications* 2017; 94: 50-68. doi: 10.1016/j.jnca.2017.06.003.
- [18] Aman M, Chua K, Sikdar B. Secure data provenance for the internet of things. In: *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*; New York, USA; 2017. pp. 11-14. doi: 10.1145/3055245.3055255.
- [19] Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K et al. ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*; Madrid, Spain; 2017. pp. 468-477. doi: 10.1109/CCGRID.2017.8
- [20] Elkhodr M, Alsinglawi B, Alshehri M. Data provenance in the internet of things. In: *Proceedings of the 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*; Krakow, Poland; 2018. pp. 727-731. doi: 10.1109/WAINA.2018.00175
- [21] Hu R, Yan Z, Ding W, Yang LT. A survey on data provenance in IoT. *World Wide Web* 2019; 23: 1441-1463. doi: 10.1007/s11280-019-00746-1
- [22] Siddiqui MS, Rahman A, Nadeem A. Secure data provenance in IoT network using bloom filters. *Procedia Computer Science* 2019; 163: 190-197. doi: 10.1016/j.procs.2019.12.100
- [23] Bertino E, Kantarcioglu M. A cyber-provenance infrastructure for sensor-based data-intensive applications. In: *Proceedings of the IEEE International Conference on Information Reuse and Integration*; San Diego, USA; 2017. pp. 108-114. doi: 10.1109/IRI.2017.91
- [24] Dogan G. ProTru: a provenance-based trust architecture for wireless sensor networks. *International Journal of Network Management* 2016; 26(2): 131-151. doi: 0.1002/nem.1925
- [25] Kamal M. Light-weight security and data provenance for multi-hop Internet of Things. *IEEE Access* 2018; 6: 34439-34448. doi: 10.1109/ACCESS.2018.2850821