Locating and Disregarding the Information from Compromised Sensors in a WSN

Zafar Iqbal and Saeid Nooshabadi
Dept. of Computer Science
Michigan Technological University
Houghton, MI, USA 49931
{zafari,saeid}@mtu.edu

Heung-No Lee
School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology
Gwangju, South Korea
heungno@gist.ac.kr

***Abstract*—Security of wireless sensor networks and reliability of the data that they generate is very critical for the intended monitoring and control applications. The information received from a sensor may be compromised because of sensor malfunction, communication link failure, or jamming attacks. This paper proposes an algorithm for locating the compromised sensor within a network of cooperating sensors and disregarding the information it sends to the base station. Thus, the final decision regarding the information collected from the sensors is less affected by the compromised sensors. This helps prevent activating wrong response mechanisms based on the compromised received information. Simulation results show that the proposed algorithm effectively locates the compromised sensors and improves the reliability of the final decision at the base station.**

***Index Terms*—Reliable communication, wireless sensor networks, trust-based algorithms, condition monitoring.**

I. Introduction

The information gathered by sensors in a wireless sensor network (WSN) is very critical to the reliable operation of the sensing-and-activation system. A compromised sensor or communication link failure leads to the reception of erroneous information which can trigger improper response mechanism. This endangers the underlying system, the associated monitoring and control applications, and most importantly human life. With the advent of the internet-of-things (IoT), physical layer security has become important to ensure the localization of compromised nodes as well as links in a network and reduce its impact on the performance of the network. The vision of IoT, ideally puts everything (systems) on the internet and therefore, vulnerable to attacks and malicious behavior. Facilities such as smart grids, nuclear installations, oil refineries, safety systems, electronic warfare systems, and autonomous vehicles are some of the major systems that can cause great damage to the economy, human life, and environment, if forced to make wrong decisions by the intruders or compromised IoT/sensor nodes.

Sensors and sensor networks are an important component of the IoT vision and are already being used in practical systems for monitoring and control applications. In the IoT world, each connected thing (system) can be seen as a sensor or a node that is a part of a larger system which is either centrally or distributively controlled. The controller is in fact influenced by the nodes, which uses the input information from these nodes and makes decisions about how these nodes should work. Therefore, the compromised or sick nodes can potentially lead to the destruction of the whole system and cause significant damage. This could be due to the communication channel outage, intrusion and hacking attacks, or malfunction of the nodes itself. Therefore, reliability of and trust on these nodes is an important factor that can be utilized to make the sensor network more secure in such situations.

Some of the recent works dealing with physical layer security and reliability challenges in industrial WSNs have been mentioned in [1] and the reliability of software defined WSNs has been discussed in [2]. The work in [3] deals with the challenges faced by energy harvesting WSNs in reliably sensing and transmitting the information to the base station (BS). A method for ensuring the reliability of the data transmitted by sensors to BS in a cooperative WSN was proposed in [4]. It uses self-healing approach to heal compromised sensors with the help of neighbouring sensors. A universal generating function (UGF) based method was proposed for cluster-based WSNs which uses weighted voting to ensure the reliability of received information [5]. The work in [6] shows that data aggregation in multi-hop sensor networks improves the reliability and energy efficiency in certain conditions. Channel and network coding techniques also play an important role in securing the transmitted information against channel errors as well as corruptions caused by intrusion and compromised nodes. The work in [7] uses optimization of energy consumption and node deployment to ensure end-to-end reliability and efficiency of data gathering in a WSN, and [8] proposes methods for data fusion in various network topologies for reliable information collection. A recent advancement in the physical layer security research is the moving target defense (MTD) theory, which increases the cost and complexity of the attacks for an attacker by reducing attack opportunities through ever-changing strategy. A solution that combines network coding and encryption for MTD has been recently proposed in [9]. Machine learning techniques can also be used to detect intrusions in an IoT node [10].

This work was supported in part by the Institute of Computing and Cybersystems (ICC) at Michigan Technological University, and in part by the National Research Foundation of Korea (NRF) Grant funded by the Korean government (MSIP) (NRF-2018R1A2A1A19018665).

978-1-5386-7693-6/18/$31.00 ©2018 IEEE

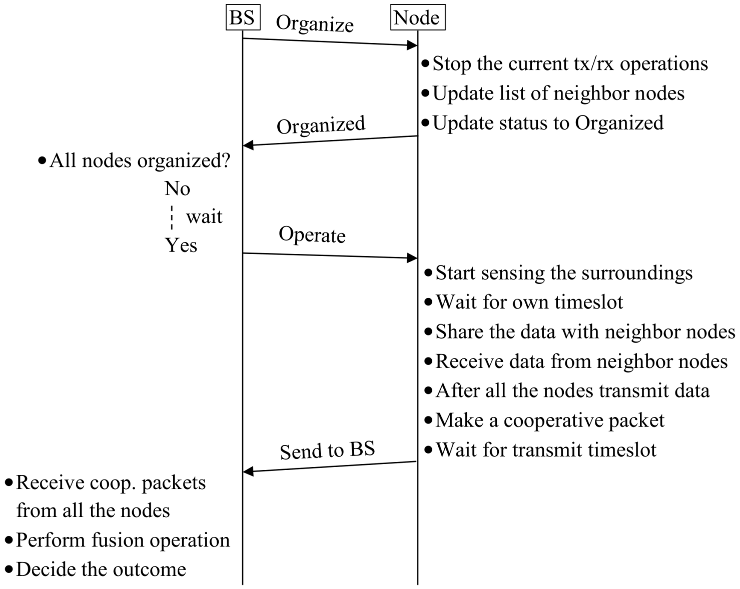
BS
Node
Organize
• Stop the current tx/rx operations
• Update list of neighbor nodes
• Update status to Organized
Organized
• All nodes organized?
No
wait
Yes
Operate
• Start sensing the surroundings
• Wait for own timeslot
• Share the data with neighbor nodes
• Receive data from neighbor nodes
• After all the nodes transmit data
• Make a cooperative packet
• Wait for transmit timeslot
Send to BS
• Receive coop. packets from all the nodes
• Perform fusion operation
• Decide the outcome

Fig. 1. Sequence flow diagram of the proposed organize and operate protocol.

This paper proposes an algorithm to locate and disregard the information received from unreliable sensors in a WSN. The proposed method uses a weighted majority-voting based fusion mechanism. In this method, each sensor is assigned a weight based on its reliability factor. If a sensor is believed to have reported wrong information, the voting weight of that sensor is reduced in the next voting phase and vice versa. Initial results of this method have been published in our previous work [11], which also considers a dual-hop cooperation mechanism using cluster heads as the relays in the second hop communication.

The rest of this paper is organized as follows. Section II desribes the system model and the proposed reliability factor feedback algorithm. Section III contains a discussion on the simulation and obtained results. Section IV concludes the paper.

II. System Model

We consider a WSN consisting of multiple sensor nodes, organized in groups of *N* nodes that cooperate with each other when transmitting their information to the BS. The network is assumed to operate in an indoor non-line-of-sight (NLOS) environment. The BS controls the operations of the network and organizes the network into a number of cooperation groups, $\mathcal{V} = \{V_i\}_{i=1}^{N}$. The sensor nodes are deployed in a static triangular grid over the area of interest, P_{AREA}, where each node has a sensing radius of r. Thus, the total number of sensors required to achieve 1-coverage, in which the entire P_{AREA} is covered by at least one sensor node, is given by $N = \frac{2P_{AREA}}{\sqrt{27}r^2}$.

To enable effective control and cooperative communication among the sensor nodes in a cooperation group, an Organize and Operate Protocol (OOP) was earlier proposed in our previous work [12]. Fig. 1 depicts the OOP with the help of a sequence flow diagram. In the OOP protocol, the BS sends an Organize message to all the nodes in the network. This message instructs the nodes to organize themselves in cooperation groups. Upon receiving this message, the nodes stop their transmit/receive operations and update their list of neighbor nodes. At this stage, the nodes update their status to organized, and responds to the BS with an ”Organized” message. After all the nodes are organized in groups, the BS then sends Operate message to the nodes. Upon receiving this message, the nodes start normal sense and transmit operations. The nodes in a cooperation group then share their sensed information with the neighboring nodes. When a node has received messages from all the nodes in the cooperation group, it makes a cooperative data packet and transmits it to the BS in its allocated timeslot. The BS, upon receiving the cooperative packets from all the nodes in the cooperation group, performs majority voting-based fusion operation and decides the outcome of the received information from the sensor nodes.

The sensing and reporting operations consists of the following phases,

1) Sensing: The sensors sense the surrounding area for the intended information i.e., temperature. Each sensor reports an alarm information of danger (D), warning (W), caution (C), and OK (O) based on temperature range from high to low, respectively.

2) Sharing with Neighbor Nodes: After sensing, every sensor shares its sensed information with its neighbouring sensors in $\mathcal{V}$ using its allocated time slot based on TDMA.

3) Transmission to BS: When all the sensors have shared their information with each other, every sensor in $\mathcal{V}$ aggregates the received information in a single packet and sends this packet to the BS using it allocated time slot based on TDMA.

We assume a network of fixed sensor nodes and therefore, do not consider issues related to the mobility of sensors. A

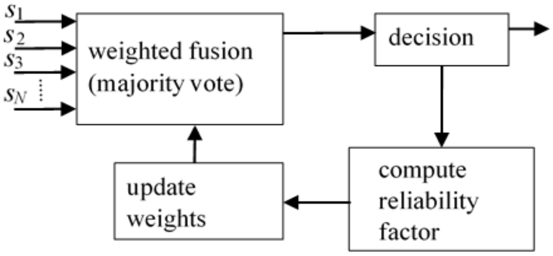

Fig. 2. Majority voting based fusion using reliability factor feedback mechanism for updating weights.

node is assumed to be able to communicate with a minimum number of neighbor nodes, 6 to 20 nodes in this work. Each node saves the source address of its neighbor nodes which is broadcasted by using a control channel. This information is used by a node when receiving the sensing data from its neighbor nodes, as it will need to decode the information received only from a sensor in its neighbor list. The BS controls the initiation and operation of the network and also update the cooperation groups periodically, depending on the application and condition of the sensor nodes.

A. Fusion Using Reliability Factor Feedback

The BS receives information from all the sensors in the cooperation group $\mathcal{V}$. Every sensor in $\mathcal{V}$ has sent a cooperative packet with aggregated information from all other sensors in the group. Thus, the received information from all the sensors in $\mathcal{V}$ makes up a matrix of size $N \times N$ where $s_{i,j}$ denotes the corresponding information from a sensor s_i sent by sensor s_j. This information is used for decision-making by applying majority-voting rule. Each sensor is assigned a weight based on its reliability factor. The majority voting based fusion is realized using weighted maximization function, which is mathematically represented as,

$$R\left(i\right) = \arg\max_{X} \sum_{j=1}^{N} w_j I\left(y_j\left(i\right) = X\right), \tag{1}$$

where j indicates the index of a sensor in the second phase, w_j is the weight associated with sensor j, $y_j\left(i\right)$ is the ith cooperative symbol received from a sensor j, and $I\left(.\right)$ is an indicator function. X = {O, C, W, D}, which is the alarm information. Therefore, $I\left(.\right)$ will return true if the received information in $y_j\left(i\right)$ is equal to one of X.

Fig. 2 shows the block diagram of the proposed fusion method which uses the reliability factor feedback mechanism. We define $\varepsilon_{i,j}$ as the corresponding reliability factor of the received information from a sensor $s_{i,j}$. To ensure high reliability of the result R, after fusion, the weights w_j are adjusted after every fusion operation as given in Algorithm 1.

III. Results and Discussion

For simulations, we consider an indoor area P_{AREA} of $100\ m \times 100\ m$, with hard partitioned walls and $N = 18$. Each node has a sensing radius of $r = 15\ m$. Rayleigh fading and lognormal shadowing, with a standard deviation $\sigma = 7$ and path-loss exponent $\eta = 3$, has been used to model the indoor environment. A carrier frequency of 2.4 GHz and

Algorithm 1 Reliability Factor Feedback Algorithm

```
$\varepsilon_{i,j} \leftarrow 0$
Loop: $i = 1$ to $N$
    Loop: $j = 1$ to $N$
    If $s_{i,j} \neq R(i)$
        $\varepsilon_{i,j} \leftarrow 1 - (\varepsilon_{i,j} + 1)/2$
    Else
        $\varepsilon_{i,j} \leftarrow 1 - (\varepsilon_{i,j})/2$
    EndIf
Loop: $j = 1$ to $N$
    $w_j = \frac{1}{NN} \sum_{i=1}^{N} \varepsilon_{i,j}$
Feedback $w_j$ to the fusion process given by (1)
```

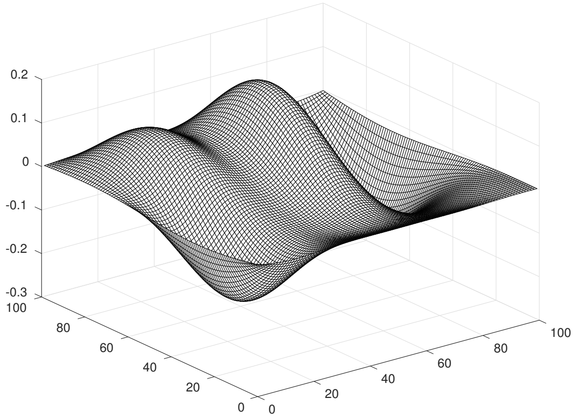

Fig. 3. Distribution of temperatures over the entire area of concern, modelled using Gaussian random field.

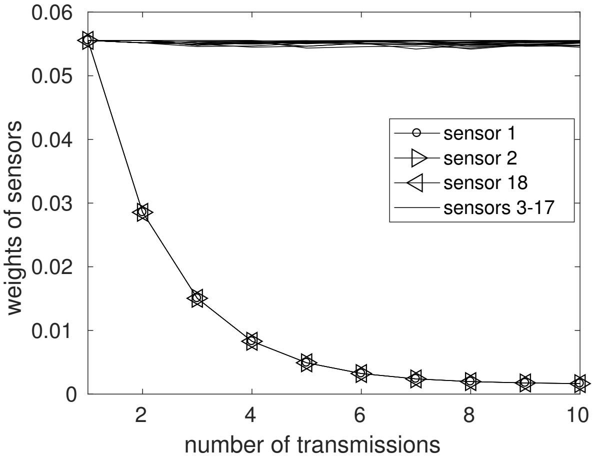

Fig. 4. Resulting weights of sensors in cooperation group, after 10 transmissions.

transmit power of 1 mW is used. The temperature is modeled over the observation area using Gaussian random field. Fig 3 depicts an instance of the distribution of temperature over the entire area of interest. The crests show higher temperature and the troughs show lower temperature at a given point. N sensors are deployed over this area in a triangular grid manner. In order to clearly observe the proposed scheme, errors were induced deliberately in the transmission from 3 sensor nodes (sensor 1, 2, and 18). The results are compared between the majority-voting based fusion scheme without the proposed weight-update mechanism, and the majority-voting based fusion scheme with the proposed weight-update mechanism in the presence of the introduced errors.

In order to verify that our proposed weight-update mechanism works correctly, we observed the performance of our proposed algorithm after each transmission at a given SNR. Fig. 4 shows the effect on the weights of sensors in $\mathcal{V}$ for 10 transmissions. It shows that the compromised sensors are easily detected and their voting weights are lowered with each transmission, which reduces its effect on the final decision. This result can be used to replace the batteries/sensors in case of defects, after successfully locating the compromised sensors. Next, we observed the behavior of our proposed algorithm when the SNR changes. Fig. 5 shows the effect on the weights of sensors after 10 transmissions at each SNR. The weights of compromised sensors have been successfully lowered at each SNR and those of correctly working sensors increase with increasing SNR because they tend to report the right information and therefore become more reliable.

To observe the effect of the proposed weight-update mechanism on the information capacity of the cooperative dual-hop communication system, we compare the mutual information curves obtained from the simulation. Fig. 6 shows the average mutual information curves at the BS for the cooperation scheme without weight update (Coop. Fusion) and cooperation using the proposed weight update method (Coop. WFusion). It shows that the proposed weight update mechanism improves the average mutual information of the system as the SNR increases and converges to 1 earlier than cooperation without weight update. This further proves that our proposed reliability factor based weight update mechanism deals with compromised sensors effectively and disregards the information received from them in the final decision-making process.

Lastly, we plot the bit-error rate (BER) curves obtained from the simulation. Fig. 7 shows the BER of the proposed cooperation scheme for 1000 senses, showing BER without weight-update mechanism (BER Fusion Sim.), the proposed weight-update mechanism (BER WFusion Sim.), relayed transmission without data aggregation, in which a node simply relays the data from a source node to BS, and direct transmission, in which no cooperation is used. We can see that the proposed method provides an improvement of about 2 dB over the cooperation without weight-update scheme at 10^{-5} and about 17 dB over both the relayed and direct communication methods at 10^{-3} BER point. The BER improves further at higher SNR.

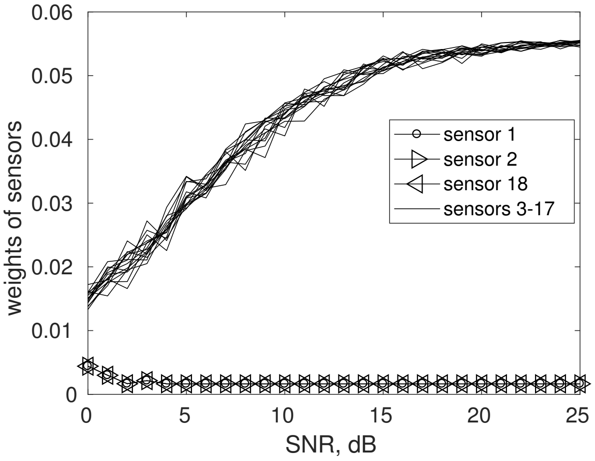

Fig. 5. Resulting weights of sensors in cooperation group, after 10 transmissions at each SNR from 0 to 25.

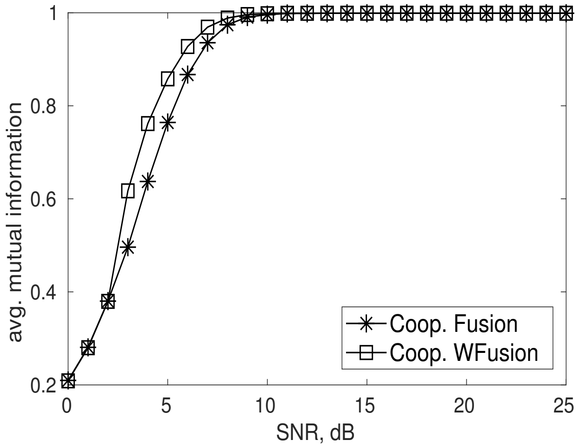

Fig. 6. Comparison of average mutual information curves of the weight update method and simple cooperation.

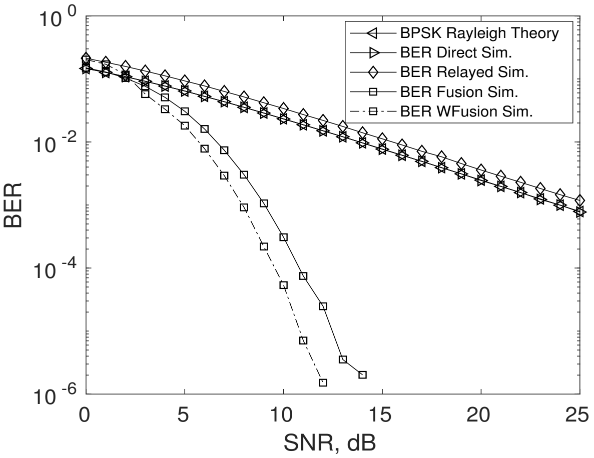

Fig. 7. Bit error rate of the proposed reliability factor feedback mechanism for cooperative transmission.

IV. Conclusion

This paper proposes a reliability factor feedback mechanism, used to update the voting weights of sensors in a dual-hop cooperative wireless sensor network. The method successfully improves the accuracy of the final decision made at the BS by effectively locating and disregarding the information received from compromised sensors. BER and mutual information curves show that the proposed method improves the performance of the cooperation scheme by effectively dealing with the compromised sensor information. As a future work, this method can be further improved to effectively locate the compromised sensors when cluster heads are used in the second hop instead of full repitition cooperation.

References

[1] J. Zhu, Y. Zou and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313-5320, 2017.

[2] Y. Lu *et al.*, "A study on the reliability of software defined wireless sensor network," *IEEE Int. Conf. on Smart City/SocialCom/SustainCom (SmartCity)*, Chengdu, pp. 129-134, 2015.

[3] L. Lei, *et al.*, "Optimal reliability in energy harvesting industrial wireless sensor networks," *IEEE Trans. Wirele. Commun.*, vol. 15, no. 8, pp. 5399-5413, 2015.

[4] A. S. Elsafrawey, E. S. Hassan and M. I. Dessouky, "Cooperative hybrid self-healing scheme for secure and data reliability in unattended wireless sensor networks," *IET Inf. Secur.*, vol. 9, no. 4, pp. 223-233, 2015.

[5] Q. Liu, H. Zhang and Y. Ma, "Reliability evaluation for wireless sensor network based on weighted voting system with unreliable links," *3rd Int. Conf. on Inf. Science and Control Eng.*, Beijing, pp. 1384-1388, 2016.

[6] S. Brown, "An analysis of loss-free data aggregation for high data reliability in wireless sensor networks," *28th Irish Sig. and Syst. Conf. (ISSC)*, Killarney, pp. 1-6, 2017.

[7] J. Long, M. Dong, K. Ota, A. Liu, and S. Hai, "Reliability guaranteed efficient data gathering in wireless sensor networks," *IEEE Access*, vol. 3, 2015, pp. 430-444, Apr. 2015.

[8] H. Luo, H. Tao, H. Ma, and S. K. Das, "Data fusion with desired reliability in wireless sensor networks," *IEEE Trans. Para. Distr. Syst.*, vol. 22, no. 3, pp. 501-513, Mar. 2011.

[9] H. Tang, Q. T. Sun, X. Yang and K. Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense," *IEEE Access*, vol. 6, 2018, pp. 26059-26068, May 2018.

[10] A. L. Buczak, E. Guven, "A survey of data mining and machine learning mehtods for cyber security intrusion detection," *IEEE Commun. Surv. and Tuto.*, vol. 18, no. 2, pp. 1153-1176, 2016.

[11] Z. Iqbal, H.-N. Lee, and S. Nooshabadi, "Highly reliable decision-making using reliability factor feedback for factory condition monitoring via WSNs," *Wireless Commun. and Mob. Comput.*, vol. 2018, Article ID 8058624, pp. 1-9 Sep. 2018.

[12] Z. Iqbal, K. S. Kim, and H.-N. Lee, "A cooperative wireless sensor network for indoor industrial monitoring," *IEEE Trans. Indust. Infor.*, vol. 13, no. 2, pp. 482-491, Apr. 2017.