EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems Research Article EAI.EU

Security-Reliability Analysis of Multi-hop LEACH Protocol with Fountain Codes and Cooperative Jamming

Dang The Hung[1], Tran Trung Duy[2,*], and Do Quoc Trinh[1]

[1] Le Quy Don Technical University, HaNoi, Vietnam
[2] Posts and Telecommunications Institute of Technology, HoChiMinh City, Vietnam

Abstract

In this paper, we investigate trade-off between security and reliability of Fountain codes (FCs) based low-energy adaptive clustering hierarchy (LEACH) networks, where the encoded packets are sent to the destination by using a cluster-based multi-hop transmission scheme with the assistance of cluster heads (CHs). With presence of an eavesdropper, a cooperative harvest-to-jam technique is employed to reduce the quality of the eavesdropping channels. Particularly, each cluster randomly selects a cluster node that generates artificial noises on the eavesdropper. For performance evaluation, we derive exact closed-form expressions of outage probability (OP) and intercept probability (IP) over Rayleigh fading channels. We then perform Monte Carlo simulations to verify the theoretical results, and compare the performance of the proposed scheme with that of the conventional LEACH scheme without using the jamming technique.

Keywords: Fountain Codes, LEACH networks, physical-layer security, cooperative jamming, outage probability, intercept probability.

Received on 23 December 2018, accepted on 31 January 2019, published on 28 March 2019

doi: 10.4108/eai.28-3-2019.157120

*Corresponding author. Email: Trantrungduy@ptithcm.edu.vn

1. Introduction

Due to low battery power, limited memory, processing and communication capabilities, performance of wireless sensor networks (WSNs), i.e., lifetime, outage probability, error rates and channel capacity, is limited. For the energy-efficiency issue, low-energy adaptive clustering hierarchy (LEACH) protocol [1]-[3] can be used to prolong the network lifetime. In LEACH, the sensor nodes are grouped into local clusters in which cluster heads (CHs) are selected to manage their own clusters in a centralized manner, i.e., gathering the data from the cluster nodes and sending to the sinks or to the neighbour CHs. Moreover, dual-hop/multi-hop relaying protocols [4]-[7] are often used to enhance the data rate, extend the network coverage, mitigate effect of fading environments and compensate the performance loss due to low transmit power and hardware imperfection.

Security is also a critical issue in WSNs due to the limited computation, memory and storage. Recently, physical-layer security (PLS) [8]-[9] has been proposed to provide security for wireless communication systems. Due to the simple implementation, PLS is suitable for WSNs [6]-[7]. To enhance secrecy performance, in terms of average secrecy capacity, secrecy outage probability and probability of non-zero secrecy capacity, the authors in [10]-[12] proposed diversity relaying protocols to enhance secrecy capacity via increasing the quality of the data links. In [13]-[14], joint cooperative relaying and jamming methods were proposed to further improve the secrecy performance. The basic idea of the cooperative jamming protocol is that friendly jammers cooperate with the legitimate receivers so that the generated interference only reduces the channel capacity of the eavesdropping links [15]-[16]. Different with [10]-[16], references [17]-[19] investigated the trade-off between security and reliability by evaluating intercept probability (IP) and outage probability (OP) of the eavesdropping and data links, respectively.

Fountain codes (FCs) [20]-[21] have gained much attention due to the simple implementation. The transmitters employing FCs can transmit a limitless

number of the encoded packets to intended receivers that can recover the original data with a sufficient number of the encoded packets. Due to broadcast of the wireless medium, the eavesdropper can easily receive the encoded packets and recover the data. Recently, FCs based secure communication protocols [22]-[25] were proposed and analysed. The authors of [22] considered the FCs based secure delivery protocol, where if the legitimate receiver can obtain sufficient number of the encoded packets before the eavesdropper, the data transmission is secure and successful. In [23], the FCs based dual-hop relaying protocol using the cooperative jamming technique was investigated. Reference [24] presented an efficient FCs-based multicast model to achieve security for Internet of Things (IoT) systems. In [25], performance of a down-link MISO scheme exploiting FCs, transmit antenna selection (TAS) and cooperative jamming was evaluated.

To the best of our knowledge, there has been no published literature related to the FCs based secure multi-hop LEACH protocol. In this paper, the source data that is encoded by FCs is sent to the destination via the intermediate clusters. To guarantee security for the data under attack of an eavesdropper, each cluster randomly selects a cluster node to realize the cooperative jamming operation. For performance evaluation and comparison, we derive exact closed-form expressions of IP and OP for the proposed protocol and the corresponding protocol without using the cooperative jamming technique, over Rayleigh fading channel. Finally, we perform Monte Carlo simulations to verify the theoretical analyses.

The rest of this paper is organized as follows. The system model of the proposed protocol is described in Section 2. In Section 3, the expressions of IP and OP are derived. The simulation results are shown in Section 4. Finally, this paper is concluded in Section 5.

2. System Model

Figure 1 presents the system model of the proposed protocol, where the source (CH of cluster 0) wants to transmit its data to the destination (CH of cluster M) via the multi-hop LEACH scenario with the assistance of multiple relays (CHs of the intermediate clusters). Using FCs, the source data is divided into L packets that are then encoded appropriately to generate the encoded packets [22]-[26]. Next, the source transmits the encoded packets to the destination. Assume that all of CHs are equipped with a single antenna, and hence the transmission of each encoded packet is performed via M orthogonal time slots, follows a time-division multiple access (TDMA) schedule.

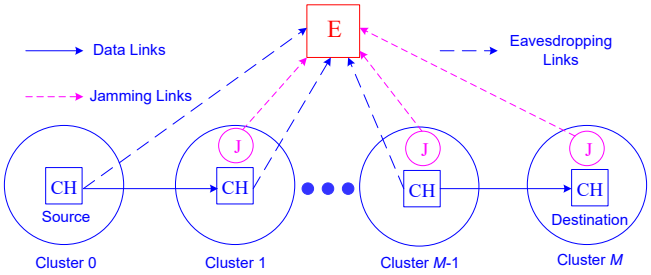

Figure 1. System model of the proposed protocol.

In the considered network, the eavesdropper (E) attempts to obtain the source data illegally. Indeed, it tries to obtain the encoded packets to recover the original data. Follows the decoding method of FCs, the destination and the eavesdropper have to receive at least H encoded packets, where $H=(1+\varepsilon)L$ and ε is the decoding overhead which depends on concrete code design [25]-[26]. Let us denote $N_{\max}$ as the maximum number of the encoded packets that the source can send to the destination, where $N_{\max} \geq H$. This means that after sending $N_{\max}$ encoded packets, the source will stop the transmission. If the destination cannot successfully receive at least H encoded packets, it cannot recover the original data, which refers to an outage event. Otherwise, the data transmission between the source and the destination is successful. For the eavesdropper, if it can receive at least H encoded packets, the source data is intercepted.

Let us denote $\gamma_{\mathrm{D},m}$ as the channel gain between CH of the $(m-1)-$th cluster and CH of the $m-$th cluster, where $m=1,2,...,M$. We also denote $\gamma_{\mathrm{E},m}$ as the channel gain between CH of the $(m-1)-$th cluster and the eavesdropper, and $\gamma_{\mathrm{J},m}$ as the channel gain between the selected jammer of the $m-$th cluster and the eavesdropper. Considering the communication at the $m-$th hop; the instantaneous signal-to-noise ratio (SNR) received at CH of the $m-$th cluster is given by

$$\psi_{\mathrm{D},m}=\frac{\alpha P\gamma_{\mathrm{D},m}}{N_0}=\alpha\Delta\gamma_{\mathrm{D},m}, \quad (1)$$

where N_0 is variance of additive white Gaussian noise (AWGN) at CH of the $m-$th cluster, P is the maximum transmit power of all of CHs, αP is the transmit power of CHs in the proposed protocol $(0.5\leq\alpha\leq 1)$ and $\Delta=P/N_0$ is transmit SNR. It is worth noting that for a fair comparison, the transmit powers of CHs and the selected jammers in the proposed protocol are αP and $(1-\alpha)P$, respectively, while that of CHs in the conventional LEACH protocol without using the cooperative jammer technique is P. Moreover, to obtain (1), it is assumed that CH of the $m-$th cluster can

perfectly remove the interference generated by the selected jammer [14], [23], [25].

Since the eavesdropper cannot remove the interference, the instantaneous signal-to-interference-plus-noise ratio (SINR) received by the node E at this hop is expressed as

$$\begin{aligned}\psi_{\mathrm{E},m} &= \frac{\alpha P\gamma_{\mathrm{E},m}}{(1-\alpha)P\gamma_{\mathrm{J},m}+N_0} \\ &= \frac{\alpha\Delta\gamma_{\mathrm{E},m}}{(1-\alpha)\Delta\gamma_{\mathrm{J},m}+1}.\end{aligned} \tag{2}$$

From (1) and (2), the instantaneous channel capacity of the data and eavesdropping links can be calculated, respectively by

$$\begin{aligned}C_{\mathrm{D},m} &= \frac{1}{M}\log_2\left(1+\psi_{\mathrm{D},m}\right) \\ &= \frac{1}{M}\log_2\left(1+\alpha\Delta\gamma_{\mathrm{D},m}\right),\end{aligned} \tag{3}$$

$$\begin{aligned}C_{\mathrm{E},m} &= \frac{1}{M}\log_2\left(1+\psi_{\mathrm{E},m}\right) \\ &= \frac{1}{M}\log_2\left(1+\frac{\alpha\Delta\gamma_{\mathrm{E},m}}{(1-\alpha)\Delta\gamma_{\mathrm{J},m}+1}\right).\end{aligned} \tag{4}$$

Next, if the cooperative jamming technique is not used, equations (3) and (4) can be rewritten, respectively by

$$C_{\mathrm{D},m} = \frac{1}{M}\log_2\left(1+\Delta\gamma_{\mathrm{D},m}\right), \tag{5}$$

$$C_{\mathrm{E},m} = \frac{1}{M}\log_2\left(1+\Delta\gamma_{\mathrm{E},m}\right). \tag{6}$$

We note that equations (5) and (6) are obtained from equations (3) and (4) by replacing α by 1. Assume that each encoded packet can be decoded successfully by CHs and the eavesdropper if the obtained instantaneous channel capacity is higher than a predetermined threshold, denoted by C_{th}. Otherwise, the encoded packet cannot be received successfully. Due to the decode-and-forward (DF) relaying method, the probability that one encoded packet can be successfully reached to the destination can be formulated by

$$\mu_{\mathrm{D}} = \prod_{m=1}^{M}\Pr\left(C_{\mathrm{D},m}\geq C_{\mathrm{th}}\right). \tag{7}$$

Next, the probability that the eavesdropper can correctly receive one encoded packet is formulated as

$$\begin{aligned}\mu_{\mathrm{E}} &= \sum_{m=1}^{M}\Pr\left(C_{\mathrm{E},m}\geq C_{\mathrm{th}}\right) \\ &\times\prod_{v=1}^{m-1}\Pr\left(C_{\mathrm{D},v}\geq C_{\mathrm{th}}\right)\Pr\left(C_{\mathrm{E},v}<C_{\mathrm{th}}\right).\end{aligned} \tag{8}$$

In (8), $\Pr\left(C_{\mathrm{E},m}\geq C_{\mathrm{th}}\right)$ is the probability that the eavesdropper can successfully receive the encoded packet at the $m-$th hop, and this event occurs when i) the transmission at the previous hops must be successful ($\Pr\left(C_{\mathrm{D},v}\geq C_{\mathrm{th}}\right), 1\leq v\leq m-1$), ii) the eavesdropper cannot obtain the encoded packet at the previous hops ($\Pr\left(C_{\mathrm{E},v}<C_{\mathrm{th}}\right), 1\leq v\leq m-1$).

We note that the probability that the destination and the eavesdropper cannot successfully receive one encoded packet is given by $1-\mu_{\mathrm{D}}$ and $1-\mu_{\mathrm{E}}$, respectively.

3. Performance Analysis

3.1. Channel Model

Assume that all of the link channels are Rayleigh fading, hence the channel gains $\gamma_{\mathrm{D},m}$, $\gamma_{\mathrm{E},m-1}$ and $\gamma_{\mathrm{J},m}$ are exponential random variables (RVs) whose cumulative distribution functions (CDFs) are given, respectively as

$$\begin{aligned}&F_{\gamma_{\mathrm{D},m}}(x)=1-\exp\left(-\lambda_{\mathrm{D},m}x\right), F_{\gamma_{\mathrm{J},m}}(x)=1-\exp\left(-\lambda_{\mathrm{J},m}x\right), \\ &F_{\gamma_{\mathrm{E},m}}(x)=1-\exp\left(-\lambda_{\mathrm{E},m}x\right),\end{aligned} \tag{9}$$

where $\lambda_{\mathrm{D},m}, \lambda_{\mathrm{E},m}$ and $\lambda_{\mathrm{J},m}$ are parameters of $\gamma_{\mathrm{D},m}$, $\gamma_{\mathrm{E},m}$ and $\gamma_{\mathrm{J},m}$, respectively, which can be modelled as in [27]:

$$\lambda_{\mathrm{D},m}=d_{\mathrm{D},m}^{\beta}, \lambda_{\mathrm{E},m}=d_{\mathrm{E},m}^{\beta}, \lambda_{\mathrm{J},m}=d_{\mathrm{J},m}^{\beta}, \tag{10}$$

where $d_{\mathrm{D},m}, d_{\mathrm{E},m}$ and $d_{\mathrm{J},m}$ are link distances between CH of the $(m-1)-$th cluster and CH of the $m-$th cluster, between CH of the $(m-1)-$th cluster and the eavesdropper, and between the chosen jammer of the $m-$th cluster and the eavesdropper, respectively.

From (9), the corresponding probability density functions (PDFs) are written by

$$f_{\gamma_{\mathrm{D},m}}(x)=\lambda_{\mathrm{D},m}\exp\left(-\lambda_{\mathrm{D},m}x\right), \tag{11}$$

$$f_{\gamma_{\mathrm{J},m}}(x)=\lambda_{\mathrm{J},m}\exp\left(-\lambda_{\mathrm{J},m}x\right), \tag{12}$$

$$f_{\gamma_{\mathrm{E},m-1}}(x)=\lambda_{\mathrm{E},m-1}\exp\left(-\lambda_{\mathrm{E},m-1}x\right). \tag{13}$$

3.2. Derivation of μ_{D} and μ_{E}

For μ_{D}, combining (3) and (7), we obtain

$$\begin{aligned}\mu_{\mathrm{D}} &= \prod_{m=1}^{M}\Pr\left(\gamma_{\mathrm{D},m}\geq\frac{\theta}{\alpha\Delta}\right) \\ &= \prod_{m=1}^{M}\left[1-F_{\gamma_{\mathrm{D},m}}\left(\frac{\theta}{\alpha\Delta}\right)\right],\end{aligned} \tag{14}$$

where

$$\theta = 2\,\hat{}\,(MC_{\mathrm{th}})-1.$$

Substituting (9) into (14), which yields

$$\mu_{\mathrm{D}} = \exp\left(-\sum_{m=1}^{M}\frac{\lambda_{\mathrm{D},m}\theta}{\alpha\Delta}\right). \tag{15}$$

For μ_E, combining (3), (4) and (8), we obtain

$$\mu_E = \sum_{m=1}^{M} \Pr\left(\frac{\alpha\Delta\gamma_{E,m}}{(1-\alpha)\Delta\gamma_{J,m}+1} \geq \theta\right) \times \prod_{v=1}^{m-1}\left[1 - F_{\gamma_{D,v}}\left(\frac{\theta}{\alpha\Delta}\right)\right] \Pr\left(\frac{\alpha\Delta\gamma_{E,v}}{(1-\alpha)\Delta\gamma_{J,v}+1} < \theta\right). \quad (16)$$

Let us consider the probability $\Pr\left(\frac{\alpha\Delta\gamma_{E,v}}{(1-\alpha)\Delta\gamma_{J,v}+1} < \theta\right)$ in (16), which is formulated as

$$\Pr\left(\frac{\alpha\Delta\gamma_{E,v}}{(1-\alpha)\Delta\gamma_{J,v}+1} < \theta\right) = \Pr\left(\gamma_{E,v} < \omega_1 + \omega_2\gamma_{J,v}\right) = \int_0^{+\infty} F_{\gamma_{E,v}}\left(\omega_1 + \omega_2 x\right) f_{\gamma_{J,v}}(x)\,dx, \quad (17)$$

where

$$\omega_1 = \frac{\theta}{\alpha\Delta}, \omega_2 = \frac{(1-\alpha)\theta}{\alpha}.$$

Plugging (9), (11) and (17) together, after some manipulations, we obtain

$$\Pr\left(\frac{\alpha\Delta\gamma_{E,v}}{(1-\alpha)\Delta\gamma_{J,v}+1} < \theta\right) = 1 - \frac{\lambda_{J,v}}{\lambda_{J,v} + \lambda_{E,v}\omega_2}\exp\left(-\lambda_{E,v}\omega_1\right). \quad (18)$$

With the same manner as deriving (18), we can write the probability $\Pr\left(\frac{\alpha\Delta\gamma_{E,m}}{(1-\alpha)\Delta\gamma_{J,m}+1} \geq \theta\right)$ in (16) as

$$\Pr\left(\frac{\alpha\Delta\gamma_{E,m}}{(1-\alpha)\Delta\gamma_{J,m}+1} \geq \theta\right) = \frac{\lambda_{J,m}}{\lambda_{J,m} + \lambda_{E,m}\omega_2}\exp\left(-\lambda_{E,m}\omega_1\right). \quad (19)$$

Substituting (9), (18) and (19) into (16), which yields

$$\mu_E = \sum_{m=1}^{M}\left(\frac{\lambda_{J,m}}{\lambda_{J,m} + \lambda_{E,m}\omega_2}\exp\left(-\lambda_{E,m}\omega_1\right)\right) \times \prod_{v=1}^{m-1}\left[\exp\left(-\frac{\lambda_{D,v}\theta}{\alpha\Delta}\right)\left(1 - \frac{\lambda_{J,v}}{\lambda_{J,v} + \lambda_{E,v}\omega_2}\exp\left(-\lambda_{E,v}\omega_1\right)\right)\right]. \quad (20)$$

If the cooperative jamming technique is not used, μ_D and μ_E can be rewritten, respectively as

$$\mu_D = \exp\left(-\sum_{m=1}^{M}\lambda_{D,m}\frac{\theta}{\Delta}\right), \quad (21)$$

$$\mu_E = \sum_{m=1}^{M}\exp\left(-\lambda_{E,m}\frac{\theta}{\Delta}\right) \times \prod_{v=1}^{m-1}\left[\exp\left(-\lambda_{D,v}\frac{\theta}{\Delta}\right)\left(1 - \exp\left(-\lambda_{E,v}\frac{\theta}{\Delta}\right)\right)\right]. \quad (22)$$

3.3. Outage Probability (OP) and Intercept Probability (IP)

As mentioned above, outage probability (OP) of the data link is defined as the probability that the destination cannot receive at least H encoded packets after the source transmitted N_{max} times. Therefore, OP can be computed by

$$\text{OP} = \sum_{t=0}^{H-1} C_{N_{max}}^{t}\left(\mu_D\right)^t\left(1-\mu_D\right)^{N_{max}-t}. \quad (23)$$

Equation (23) implies that after the source stops the transmission, the destination only receives t encoded packets, where $0 \leq t \leq H-1$.

Let us consider the intercept probability (IP), which can be calculated as

$$\text{IP} = \sum_{w=H}^{N_{max}} C_{N_{max}}^{w}\left(\mu_E\right)^w\left(1-\mu_E\right)^{N_{max}-w}. \quad (24)$$

In (24), since the eavesdropper can obtain w encoded packets, where $H \leq w \leq N_{max}$, it can recover the original data of the source, and hence the source data is intercepted.

4. Simulation Results

In this section, we present Monte-Carlo simulations to verify the theoretical results shown in Section 3 as well as to compare the performance of the proposed protocol (denoted by Jam) and that of the conventional LEACH protocol (denoted by Non). In the simulation environment, a two-dimensional Oxy plane is considered, where all of the nodes in the $m-$th cluster is located at ($m/M, 0$) and the eavesdropper is placed at (0.5, 0.5), where $m = 0,1,...,M$. In all of the simulations, we fix the path-loss exponent (β) by 3, and the target rate (C_{th}) by 1.

In Figs. 2-3, we present OP and IP as a function of the transmit SNR (Δ) in dB. In these figures, the fraction α is fixed by 0.85, and the values of H and N_{max} are assigned by 5 and 7, respectively. In Fig. 2, we see that the OP values decrease with the increasing of Δ. Moreover, OP of the proposed protocol (Jam) is higher than that of the non-jamming protocol (Non) because the transmit power of CHs in the non-jam protocol is higher. As we can see, the performance loss is about 1dB. It is also seen from Fig. 2 that the OP performance of the

considered protocols is worse with higher number of hops. In Fig. 3, the IP values rapidly increase with the increasing of Δ, and IP of the proposed protocol is much lower than that of the Non protocol. In addition, the IP values decrease with higher number of hops between the source and the destination (M). Finally, it is worth noting that the simulation results (Sim) match very well with the theoretical ones (Theory), which validates the formulas derived in Section 3.

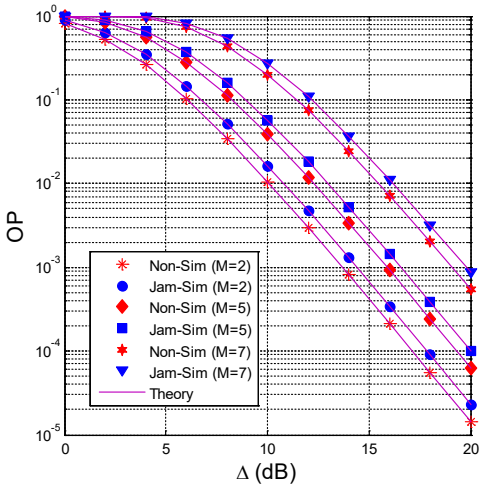

Figure 2. OP as a function of Δ dB when $\alpha = 0.85$, $H = 5$, $N_{\max} = 7$.

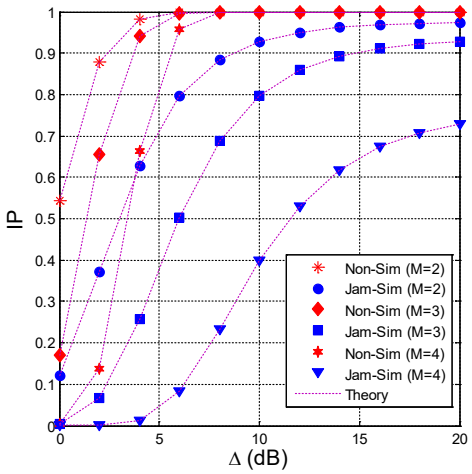

Figure 3. IP as a function of Δ dB when $\alpha = 0.85$, $H = 5$, $N_{\max} = 7$.

Figures 4 and 5 present OP and IP as a function of M with different values of α. Again, the OP performance of the Non protocol is better than that of the proposed protocol, but the IP performance of the Non protocol is much worse. As seen in Fig. 5, the source data in the Non protocol is almost intercepted by the eavesdropper. For the proposed protocol, the IP values decrease with the decreasing of α because the transmit power of the selected jammers increases. However, decreasing the value of α will decrease the transmit power of CHs, resulting in the OP performance degradation. In Figs. 4-5, it can be observed that when $M = 2$, the value of OP (IP) is lowest (highest). Again, the simulation results verify the theoretical ones.

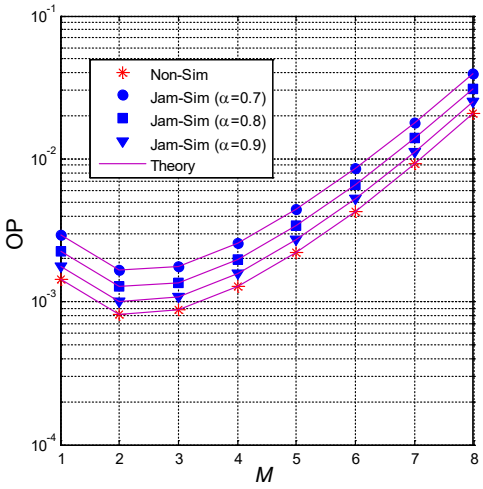

Figure 4. OP as a function of M when $\Delta = 20$ dB, $H = 5$, $N_{\max} = 6$.

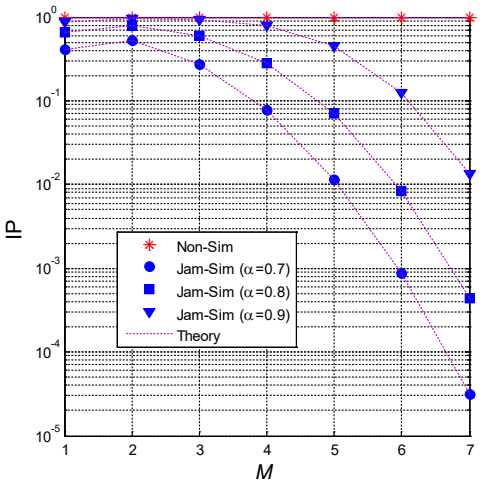

Figure 5. IP as a function of M when $\Delta = 20$ dB, $H = 5$, $N_{\max} = 6$.

Figures 6 and 7 investigate the trade-off between IP and OP with different values of H and $N_{\max}$. As we can see in Fig. 6, the OP performance of the considered protocols is better as H decreases and $N_{\max}$ increases. Indeed, with lower value of H and higher value of $N_{\max}$, the probability that the destination can receive sufficient number of the encoded packets increases, which reduces the outage probability. However, as illustrated in Fig. 7, the IP values also increase as H decreases and $N_{\max}$ increases. Therefore, the values of H and $N_{\max}$ should be designed appropriately to guarantee QoS (OP) and security (IP). For example, in the proposed protocol, to satisfy the required QoS of $\text{OP} \le 0.01$ and the security level of $\text{IP} \le 0.1$, we have to set the values of H and

N_{max} by 4 and 9, respectively. Finally, we again see that the simulation and theoretical results are in a good agreement.

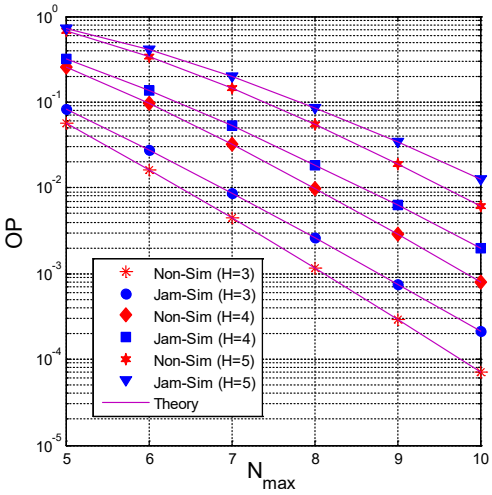

Figure 6. OP as a function of N_{max} when $\Delta = 7.5\,\text{dB}$, $\alpha = 0.85,\ M = 5.$

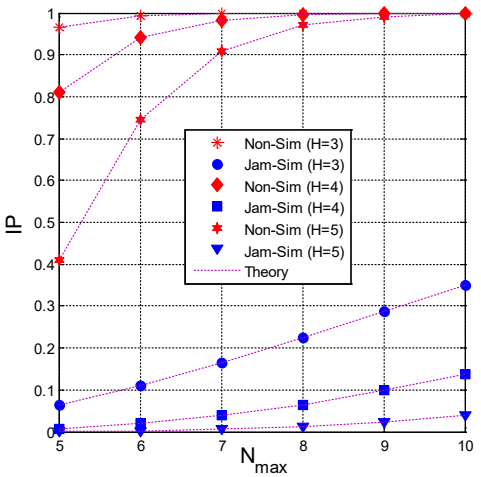

Figure 7. IP as a function of N_{max} when $\Delta = 7.5\,\text{dB}$, $\alpha = 0.85,\ M = 5.$

5. Conclusion

In this paper, we proposed the FCs-based multi-hop LEACH protocol using cooperative jamming technique for the reliable and secure communication in WSNs. The system performance such as OP and IP was evaluated via both Monte Carlo simulations and theoretical analyzes. The obtained results showed that there exists a trade-off between security and reliability. Therefore, the system parameters such as the number of hops, the fraction of the transmit power allocated for generating the artificial noises, the number of encoded packets required for recovering the source data, and the maximum number of transmission times at the source should be carefully designed so that the proposed protocol can guarantee both security and QoS.

Acknowledgements

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.317.

References

[1] Asaduzzaman and H. Y. Kong (2010) Energy Efficient Cooperative LEACH Protocol for Wireless Sensor Networks. *Journal of Communications and Networks*, **12** (4): 358 – 365.

[2] T. T. Duy and H. Y. Kong (2015) Secrecy Performance Analysis of Multihop Transmission Protocols in Cluster Networks. *Wireless Personal Communications*, **82** (4): 2505-2518.

[3] S. K. Singh, P. Kumar, and J. P. Singh (2017) A Survey on Successors of LEACH Protocol. *IEEE Access*, **5**: 4298 – 4328.

[4] T. T. Duy, T. Q. Duong, D.B. da Costa, V.N.Q. Bao, and M. Elkashlan (2015) Proactive Relay Selection with Joint Impact of Hardware Impairment and Co-channel Interference. *IEEE Transactions on Communications*, **63**(5): 1594-1606.

[5] F. S. Al-Qahtani, R. M. Radaydeh, S. Hassan, T. Q. Duong, and H. Alnuweiri (2017) Underlay Cognitive Multihop MIMO Networks With and Without Receive Interference Cancellation. *IEEE Transactions on Communications*, **65**(4): 1477 – 1493.

[6] J. A. Bengua, H. D. Tuan, T. Q. Duong, and H. Vincent Poor (2018) Joint Sensor and Relay Power Control in Tracking Gaussian Mixture Targets by Wireless Sensor Networks. *IEEE Transactions on Signal Processing*, **66**(2): 492 – 506.

[7] T. D. Hieu, T. T. Duy, and B.-S. Kim (2018) Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises. *IEEE Sensors Journal*, **18**(12): 5173 - 5186.

[8] P. K. Gopala, L. Lai, and H. E. Gamal (2008) On the Secrecy Capacity of Fading Channels. *IEEE Transactions on Information Theory*, **54**(10): 4687-4698.

[9] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty (2015) Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond. *IEEE Communications Magazine*, **53**(12): 32 – 39.

[10] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao (2015) Secrecy Performance Analysis with Relay Selection Methods under Impact of Co-channel Interference. *IET Communications*, **9**(11): 1427-1435.

[11] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang (2017) Secure Full-Duplex Spectrum-Sharing Wiretap Networks With Different Antenna Reception Schemes. *IEEE Transactions on Communications*, **65**(1): 335 – 346.

[12] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis (2017) Secrecy Cooperative Networks With Outdated Relay Selection Over Correlated Fading Channels. *IEEE Transactions on Vehicular Technology*, **66**(8): 7599 – 7603.

[13] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and Trung Q. Duong (2015) Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wireless Communications Letters*, **4**(1): 46-49.

[14] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu (2017) Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer. *IEEE Wireless Communications Letters*, **6**(2): 174-177.

[15] N.-P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and K. Tourki (2018) Secure Massive MIMO With the Artificial Noise-Aided Downlink Training. *IEEE Journal on Selected Areas in Communications*, **36**(4): 802 – 816.

[16] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney (2016) Optimal Transmission With Artificial Noise in MISOME Wiretap Channels. *IEEE Transactions on Vehicular Technology*, **65**(4): 2170 - 2181.

[17] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo (2015) Relay-Selection Improves the Security-Reliability Trade-off in Cognitive Radio Systems. *IEEE Transactions on Communications*, **63**(1): 215–228.

[18] Y. Zou (2017) Physical-Layer Security for Spectrum Sharing Systems. *IEEE Transactions on Wireless Communications*, **16**(2): 1319 – 1329.

[19] P. M. Nam, T. T. Duy, and P. V. Ca (2019) End-to-end Security-Reliability Analysis of Multi-hop Cognitive Relaying Protocol with TAS/SC-based Primary Communication, Total Interference Constraint and Asymmetric Fading Channels. *International Journal of Communication Systems*, **32**(2): 1-18.

[20] D. J. C. Mackay (2005) Fountain Codes. *IEE Proceedings - Communications*, **152**(6): 1062-1068.

[21] J. Castura and Y. Mao (2006) Rateless Coding over Fading Channels. *IEEE Communications Letters*, **10**(1): 46-48.

[22] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du (2014) Exploiting Fountain Codes for Secure Wireless Delivery. *IEEE Communications Letters*, **18**(5): 777-780.

[23] L. Sun, P. Ren, Q. Du, and Y. Wang (2016) Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, **12**(1): 291-300.

[24] Q. Du, Y. Xu, W. Li, and H. Song (2018) Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes. *Wireless Communications and Mobile Computing*, Article ID **8404219**: 1-11.

[25] D. T. Hung, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao (2018) Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments. *In Proceeding of of the 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom2018)*, HoChiMinh city, VietNam, 164-169.

[26] J. Castura and Y. Mao (2007) Rateless Coding for Wireless Relay Channels. IEEE Transactions on Wireless Communications, **6**(5): 1638-1642.

[27] J. N. Laneman, D. N. Tse, and G. W. Wornell (2004) Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. IEEE Transactions on Information Theory **50**(12): 3062 - 3080.