JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 33, 1055-1067 (2017)
DOI: 10.6688/JISE.2017.33.4.13

Short Paper

Secret Data Transmission in Wireless Sensor Network with Physical Layer Network Coding

QIAO LIU, YONG WANG, WENJING ZHANG AND HUI LI
ISN, School of Cyber Engineering
Xidian University
Xi'an, 710071 P.R. China
E-mail: {windachilles; xd.zhangwenjing}@gmail.com; {wangyong; lihui}@mail.xidian.edi.cn

In this paper, the physical layer network coding is applied into wireless sensor network for secret data transmission. The source node will send the gathered data to the sink node with help of multiple relay nodes. By applying the physical layer network coding, the received signal at the relay nodes is guaranteed to be a summed signal which cannot be separated. Thus, the attack from untrusted relays as well as external eavesdroppers can be prevented. Two types of coding algorithm has been discussed, one for BPSK coding and another for nested lattice coding. Analysis is also conduct for the proposed protocol. In the view of transmission, the proposed protocol can achieve the same time slots cost as the non-security protocol. In the view of security, the proposed protocol can successfully against the attacks identical with cryptography approach, however less hardware and computational complexity will be consumed for the proposed protocol.

Keywords: WSN, multiple hops transmission, physical layer network coding, nested lattice code, physical layer security

1. INTRODUCTION

With the development of the information and communication technology, the age of smart is coming. Smart phone, smart vehicle, smart grid, so many fields is becoming smarter and smarter to provide more convenient service for people. For the improvement of the city living, the concept of smart city is proposed integrated a lot of emerging information and communication technologies. Among these technologies, wireless sensor network (WSN) is the enabling technique for the Internet of Things (IoT) which is one of the most important platforms of smart city.

The wireless sensors network enables a lot of distributed sensor node to monitor data, and then transmit the data to the sink node for further processing. For the wireless sensor network, the researchers have focused on the topics of efficient data gathering [5], network structure [2], and routing protocol [13]. Besides these, the security issue is one of the most important topics for WSN especially when WSN is applied into healthy application or industry application. However, due to the wireless transmission feature and distribution system structure, WSN is confronted with a lot of attacks including eaves-

Received June 29, 2016; revised August 4, 2016; accepted October 11, 2016.
Communicated by Zhe Liu.

dropping attack, Denial of Service (DoS) attack, jamming attack, hole attack, Sybil attack and so on, the readers may refer [1, 4] for more details.

Two noteworthy features should be considered to prevent the former mentioned different attacks. In one hand, all the nodes in WSN are in low power and low cost. Although this fact guarantee the network is designed in a cost efficient way, it also leads to the very low computation capability of the WSN nodes. In another hand, the lack of authentication central result in the hardness of key distribution in WSN. To deal with the first problem, some researchers focus on the application of light weight cryptography [7-10] or lightweight authentication [3, 15] in WSN. However, all these approaches are all based on the shared key, which will suffer the second hard problem. Thus, it is desirable to secure WSN in a brand new prospect.

Physical layer network coding is usually designed for the improvement of transmission efficiency, further in some recent works, the physical layer network coding is also considered to secure the data exchange. The discussion is first for 2-hop, *i.e.* two-way relay channel [6, 12], then for the multi-hop with bi-relaying [14]. All these works enjoy the benefit of key sharing needlessness which is the common feature of physical layer security approaches.

Although the former mentioned works concentrate on the two way data exchange, they motivate us to propose a novel secure physical layer network coding protocol for one way data transmission. Thus, in this paper we apply the physical layer network coding into WSN. We consider on source node send its gathered data to the sink node. By applying the physical layer network coding, the received signal at either the relay node or eavesdroppers is a summed signal of data and a pseudorandom sequence, so these nodes cannot distinguish the data. In this way, the transmission progress is secure without a shared key.

The contribution of this work is listed as:

- Firstly, we apply the physical layer network coding into the simplest transmission model, *i.e.*, 2-hop transmission. Two different kind of coding algorithm has been discussed including BPSK coding and nested lattice coding.
- Secondly, based on the discussion in 2-hop transmission, we extend the physical layer network coding into general n-hop. By optimizing the time slots cost in the most efficient way, the security is achieved in least trade-off of hardware and computational complexity.
- Finally, analysis of the proposed protocol has been conduct in the terms of transmission and security. For the transmission, we show the proposed protocol enjoys transmission efficiency than the cryptography approach. For the security, we show the proposed protocol can be successfully against the attack from untrusted relay nodes as well as external eavesdroppers.

The rest of this paper is organized as: the system model is introduced in the second section. In section 3, the physical layer network coding for 2-hop transmission has been proposed with two coding algorithm including BPSK coding and nested lattice coding. The protocol has been extended into general n-hop in section 4. Finally, the conclusion is given in the last section.

2. SYSTETEM MODEL

In this section, we will introduce the system model for transmission from the source node to the sink node. Following the transmission model, we will discuss the two types of attack through the transmission path.

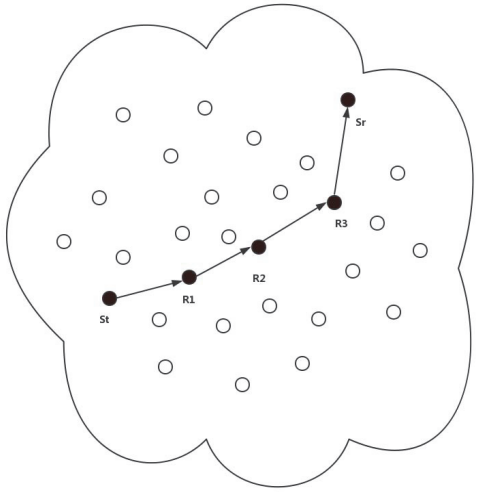

Fig. 1. System Model. S_t is the source node, S_r is the sink node. R_i is the relay node. $\rightarrow$ is the transmission path from the source node to the sink node in Wireless Sensor Network.

2.1 Transmission Model

In this work, we consider the transmission model that one source sensor node sends its gathered data to the sink node with help of multiple relay nodes. The source sensor node, acting as the transmitter in the transmission scheme, is named as S_t, and sink node is named as S_r. The source node, sink node and the relay nodes form the one path for the transmission. The relay nodes are chosen by the routing protocol, the readers can refer [16, 17] to obtain the detail of the protocol. This model has been depicted in Fig. 1.

Assuming the sink node is in the nth hop of the source node, so there are $n-1$ relay nodes to assistant the transmission. The relay nodes are named as $R_i(i = 1, 2, \ldots, n-1)$ if this relay is in the ith hop of the source nodes.

Each node are assumed to only connect with its neighbor nodes, *i.e.*, the source node S_t only share transmission channel with R_1, R_1 share transmission channel with S_t and R_2, *etc.* For simplicity, we name the channel with the direction to the sink node as right link channel and the channel to the source node direction as left link channel. The channel is named as h_{ij}, for i is the transmitter and j is the receiver. For example, the right link channel from source node S_t to R_1 is $h_{S_tR_1}$.

In traditional transmission scheme, the data from the source node will be right link forward to the sink node costing n time slots which is a minimized number. However, physical layer secrecy cannot be provided with the traditional scheme which means that the security of such protocol is only based on the cryptography. As mentioned previously, the key distribution is still a hard problem in WSN, so the trade-off between the time

slots cost and security is necessary.

The sink node and the relay nodes are required to employ a pseudorandom sequence generator (PRSG). In each round of data transmission, the generated pseudorandom sequence must be different. These sequences are nonpublic, so only the nodes themselves can know their own sequences.

Finally, we assume perfect synchronization can be achieved in our work. For the asynchronous scenario, physical layer network coding has been discussed in [11].

2.2 Security Model

Besides the source node, sink node and relay nodes, there are also existing other nodes in the network. Except the source node and sink node, all other nodes including the relay nodes can be considered as potential threaten for which is eager to wiretap the data. Following, we will discuss the two types attack from either relay nodes or non-relay nodes.

Relay Nodes Attack

We first consider the attacks from the relay nodes. The relay nodes are acting two roles in this situation. In one hand, the relays will obey the protocol to accomplish the data transmission. In another hand, the relays are curious about the data, so they will do their best to recover it. This model is often referenced as *honest-but-curious* model.

In this work, we only consider the relay can launch the passive attack. Thus, the relay nodes are not able to rewrite the data, and they are not able to require extra information rather its received signal.

The neighbor colluding between the relay nodes are forbidden in the network, *i.e.*, all the relay nodes will not share any information with others. Similarly, relay nodes are not allowed to collude with the non-relay nodes.

Non-Relay Nodes Attack

Besides the helper nodes, the nodes outside the path in the network can be divided into two categories, one group of decent nodes and another group of wiretap nodes. The nodes are named as wiretap nodes because they are acting as the wiretappers for the transmitted data.

The wiretap nodes are assumed to only can launch the passive attacks. Thus, they will not try to block the transmission, however, they will collect the information from the wireless medium and try to recover the transmitted data. This is a standard assumption for most physical layer security schemes.

Colluding is not allowed between the wiretap nodes, and as former mentioned colluding is not allowed between wiretap nodes and relay nodes either.

3. PHYSICAL LAYER NETWORK CODING PROTOCOL FOR 2-HOP TRANSMISSION

In this section, we will consider the simplest situation, *i.e.*, 2-hop transmission. There are three nodes in the 2-hop transmission, the source node S_t, the sink node S_r, and one relay node R.

Two time slots are cost to accomplish one round of information transmission. In the first time slot, S_t send its message c_t and S_r send the generated pseudorandom sequence c_r to the relay node. The message or sequence is in binary value. These two signals will be perfect synchronized as former mentioned to form a summed signal. In the second time slot, the relay node sends the summed signal to S_r and S_r recovers c_t with help of c_r.

Two types of physical layer network coding schemes will be introduced, one is the simplest scheme *i.e.*, BPSK scheme, and another is nested lattice code scheme.

3.1 BPSK Physical Layer Network Coding in 2-hop Transmission

Before the first time slot, the source node and sink node will first encode the message or pseudorandom sequence to the transmitted signal X_t to X_r by modulating 0 to −1 and 1 to +1. After the encoding, the source node and sink node transmit the coded signal to the relay as:

$$Y_R = h_{s_t R} \cdot X_t + h_{s_r R} \cdot X_r + n_R, \tag{1}$$

where n_R is the zero mean circularly symmetric complex Gaussian noise as $n_R \sim CN(0, \delta)$. By using signal processing technique, this received signal can form the summed signal as:

$$\tilde{Y}_R = (X_t + X_r) + n'_R, \tag{2}$$

where n'_R is the resulting noise. The relay then decodes the summed signal back to binary by the mapping rule as:

$$\tilde{Y}_R = \begin{cases} 1, & \left|\tilde{Y}_R\right| < 1 + \ln 2 / 2 \\ 0, & otherwise \end{cases}. \tag{3}$$

From the view of binary field, the decoded signal $\tilde{Y}_R$ is the binary XOr of c_t and c_r as:

$$\tilde{Y}_R = c_t \oplus c_r, \tag{4}$$

The progress to obtain such XOr signal is denoted as Alignment Progress which will be used in the general n-hop transmission.

After the decoding, the relay will encode such XOred signal $\tilde{Y}_R$ with the same encoding algorithm to its own transmitting signal X_R. Then, relay node will forward this signal to the sink node as:

$$\tilde{Y}_{S_r} = h_{Rs_r} \cdot X_R + n_{S_r}. \tag{5}$$

Similarly, n_{S_r} is the noise at the sink node. By using BPSK demodulating, the sink node decoding Y_{S_r} back to the binary XOr $c_t \oplus c_r$. Thus, the sink node can recover the message c_t from the source node.

This progress is shown in Fig. 2.

In addition, we introduce the traditional cryptography approach for the 2-hop as a comparison. In cryptography approach, the key negotiation will be conducted before the transmission to generate the shared key K. With the key K, S_t will encrypt its data and send to R_1, and R_1 forward the encrypted data to S_r. However, as former mentioned, the key negotiation is hard to deployed especially considering the relay nodes are untrusted. Further the key negotiation will cost additional computational and hardware complexity. These reasons are also the motivation of the proposed physical layer network coding scheme. The progress of cryptography approach is shown in Fig. 3.

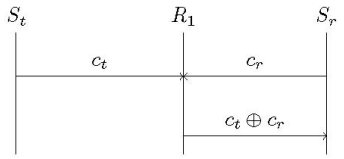

Fig. 2. Physical layer network coding approach for 2-hop transmission.

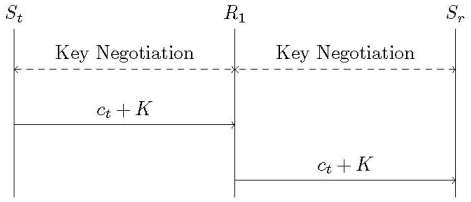

Fig. 3. Cryptography approach for 2-hop transmission.

3.2 Nested Lattice Physical Layer Network Coding in 2-hop Transmission

The BPSK physical layer network coding scheme is the simplest scheme, however, the transmission performance improvement can be achieved with little computational and hardware complexity trade-off, *i.e.*, nested lattice coding scheme.

Basic Conceptions and Notations for Lattice and Nested Lattice Code

Lattice Λ: The lattice is defined as a set of points (or vectors) which are the linear combinations of the basis vectors. If the basis vectors are real number basis, the lattice is called real lattice. If the basis vectors are complex basis, the lattice is called complex lattice. This can be explained as:

$$\Lambda = \{\mathbf{z}\mathbf{G}_\Lambda : \mathbf{z} \in \mathbb{Z}^n\}, \tag{6}$$

where $\mathbf{G}_\Lambda$ is the generator matrix for Λ formed by the basis $g_1, g_2, \cdots, g_n$ as: $G_\Lambda \triangleq \left[g_1^T \mid g_2^T \mid \cdots \mid g_n^T \right]^T$.

Nearest Point Quantize $\mathcal{Q}_\Lambda$: The quantize will send the point not in the lattice set to the nearest lattice point in Euclidean distance.

Voronoi Region $\mathcal{V}_\Lambda(\lambda)$: The Voronoi Region of a lattice point λ is defined as the set of points which will be quantized to itself as:

$$\mathcal{V}_\Lambda(\lambda) \triangleq \left\{ x \in \mathbb{C}^n : Q_\Lambda(x) = \lambda \right\}. \tag{7}$$

Particularly, the Voronoi Region of the original is called the Fundamental Region $\mathcal{R}_\Lambda$ as:

$$\mathcal{R}_\Lambda(\lambda) = \mathcal{V}_\Lambda(0). \tag{8}$$

Nested Lattice: The nested lattice is defined as the coarse lattice Λ_{coarse} is the sub-lattice of the fine lattice Λ_{fine}.

Nested Lattice Code $\mathcal{L}$: The nested lattice code is defined as the set of all co-set leaders in $\Lambda_{fine}/\Lambda_{coarse}$. Geometrically speaking, the codeword of nested lattice is the set of points of the fine lattice that lie within the fundamental region of the coarse lattice as:

$$\mathcal{L}\left(\Lambda_{fine}, \Lambda_{coarse}\right) = \Lambda_{fine} \bmod \Lambda_{coarse} = \Lambda_{fine} \cap \mathcal{V}_{\Lambda coarse} \ . \tag{9}$$

Example: We give an complex nested lattice code built as: $\Lambda_{fine} = \mathbb{Z}[i]$ and $\Lambda_{coarse} = 2\mathbb{Z}[i]$. This has been shown in Fig. 4.

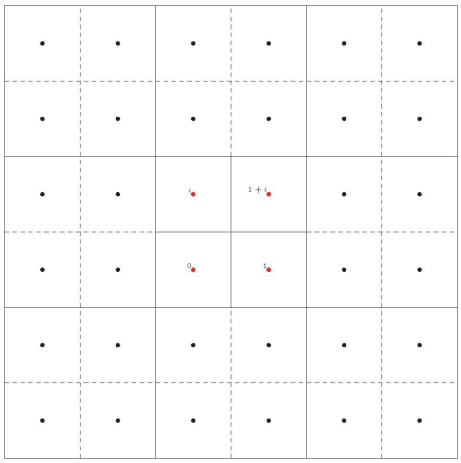

Fig. 4. An example of nested lattice code with $\Lambda_{fine} = \mathbb{Z}[i]$ and $\Lambda_{coarse} = 2\mathbb{Z}[i]$.

Nested Lattice Encoding at Source Node and Sink Node

The nested lattice code will be conducted for the source node and sink node. The source node will encode the message as: φ: $c_t \rightarrow \mathcal{L}$ which is a mapping from the message to the codeword. Similarly, the sink node will also conduct nested lattice encoding by mapping its pseudorandom sequence to the codeword φ: $c_r \rightarrow \mathcal{L}$.

Recall the example in the last subsection, the encoding mapping will map two successive bits from c_t or c_r to the codeword. We show the mapping from two bits of c_t to codeword as:

$$\varphi(c_t) = c_t(n)+c_r(n+1)i. \tag{10}$$

After this mapping, the source node and sink node generate transmitted signal X_t and X_r.

Nested Lattice Decoding at Relay Node

The relay node will receive the aligned signal $\widetilde{Y}_R$ identical with Eq. (2), then the relay will obtain the codeword sum of c_t and c_r from $\widetilde{Y}_R$ by nested lattice decoding. The decoder will send the sum signal by Nearest Point Quantize defined in the last subsection as:

$$\begin{aligned} \hat{Y}_R &= \widetilde{Y}_R && \bmod \Lambda_{coarse} \\ &= (c_t \oplus c_r) + Z_v && \bmod \Lambda_{coarse}. \end{aligned} \tag{10}$$

Taking the same example, we show this progress as Fig. 5. In this example, the transmitted two bits for source node are 01, so the encoded signal is i for source node. The two bits of pseudorandom sequence generated in S_r are 11, so the nested lattice code word is $1+i$. After the decoding algorithm, decoded signal is 1 which is $c_t \oplus c_r$.

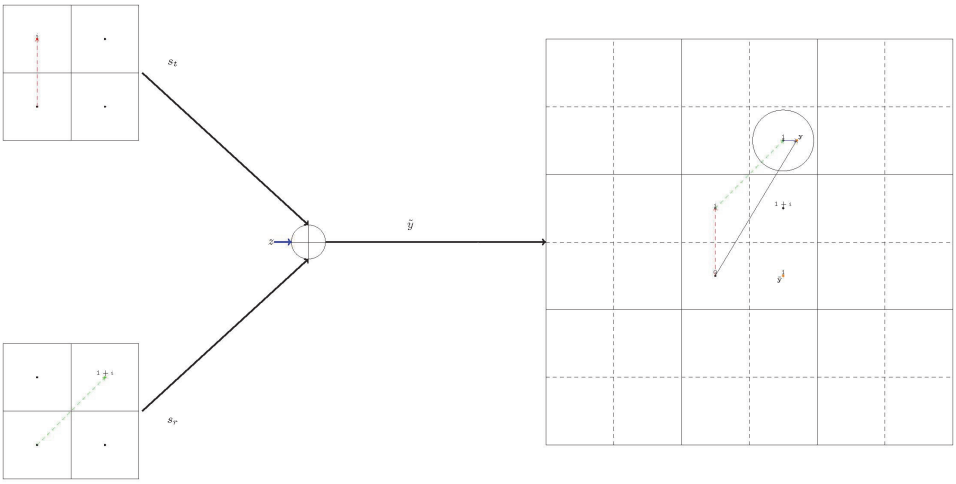

Fig. 5. A decoding example at relay nodes with nested lattice code.

Relay Forwarding

After the decoding in the relay node, relay will forward the summed codeword to the sink node. After the transmission, the sink node will first conduct the inverse mapping of the encoding to back the codeword to the binary field. Then do XOr operation with its own pseudorandom sequence to recover the data.

In the example in the previous discussion, the relay will forward 1 to the sink node. Then the sink node inverse map 1 to 10. Recall the generated pseudorandom sequence is 11, so the transmitted data from source node is 01. Thus, one round of data transmission is completed with nested lattice code in 2-hop.

4. PHYSICAL LAYER NETWORK CODING PROTOCOL FOR GENERAL *N*-HOP TRANSMISSION

Based on the discussion for the 2-hop transmission, we generalize the physical layer network coding into *n*-hop. We will not distinguish which coding algorithm will be applied for *n*-hop case, instead we use $\mathcal{E}()$ to denote the encoding and $\mathcal{D}()$ to denote the decoding.

4.1 *n*-hop Transmission Protocol

For *n*-hop, *n*+1 time slots are needed to finish one round of transmission, and then we will introduce the whole transmission in detail.

Time Slot 1: In the first time slot, the source node S_t will conduct Alignment Progress with relay node R_2 at R_1. Before transmitting, S_t will encode the message data and R_2 encode its pseudorandom sequence as:

$$\textit{Encoding: } X_t = \mathcal{E}(c_t),\ X_{R_2} = \mathcal{E}(c_2). \tag{12}$$

Then these two nodes send the coded message to R_1 as:

$$Y_{R_1} = h_{s_t R_1} X_t + h_{R_2 R_1} X_2 + n_{R_1}. \tag{13}$$

With help of signal processing techniques, the resulting received signal at R_1 is:

$$\tilde{Y}_{R_1} = \left(X_t + X_{R_2}\right) + n'_{R_1}. \tag{14}$$

Then R_1 obtain the summed signal by decoding as:

$$\textit{Decoding: } \hat{Y}_{R_1} = \mathcal{D}(\tilde{Y}_{R_1}) = c_t \oplus c_2 \tag{15}$$

$\hat{Y}_{R_1}$ will be the transmitted message of R_1 for the next time slot.

Time Slot 2: In the second time slot, R_1 will align $c_t \oplus c_2$ with c_3 from R_3 at R_2. The transmitting progress is identical with Time Slot 1, and after the decoding R_2 will receive summed signal $c_t \oplus c_2 \oplus c_3$.

Time Slot 3 to Time slot *n*–2: From the time Slot 3 to Time Slot *n*–2, the transmission progress is identical with the Time Slot 2.

Detailed to say, relay node R_i will align $c_t \oplus c_{r+1}$ with c_{i+2} from R_{i+2} at R_{i+1}. With received $c_t \oplus c_{i+1} \oplus c_{i+2}$, R_{i+1} subtract c_{i+1} and prepare to align $c_t \oplus c_{i+2}$ in the next time slot.

Time Slot *n*−1: In this time slot, the relay node R_{n-2} will conduct Alignment Progress with the sink node S_r at the last relay node R_{n-1}. After decoding, R_{n-1} will obtain $c_t \oplus c_{n-1} \oplus c_r$. By subtracting its own pseudorandom sequence, the sum $c_t \oplus c_r$ can be obtained.

Time Slot *n*: This time slot is the last time slot of whole transmission. In this time slot, the last relay node R_{n-1} will forward obtained $c_t \oplus c_r$ to the sink node. This progress is identical with the second time slot of the 2-hop transmission.

After the forward, sink node S_r obtain $c_t \oplus c_r$, then S_r recover c_t with help of its own pseudorandom sequence c_r. Thus, one round of transmission is completed.

We give an example of the proposed protocol in Fig. 6. We consider the sink node is in the 4-hop of the source node, so three relay nodes will assistant the transmission.

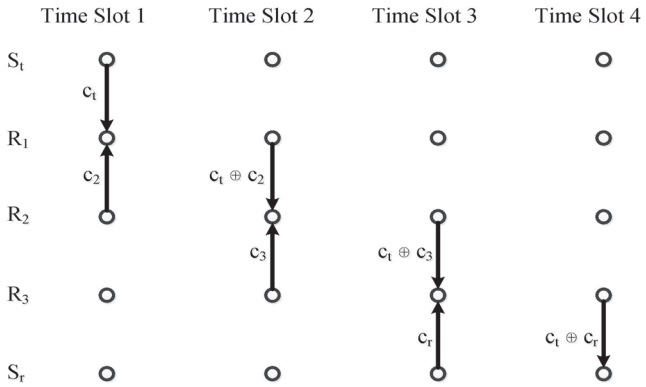

Fig. 6. The protocol example for 4-hop transmission.

4.2 Transmission Performance Analysis

If the security issues are not in consideration, all the relay node will forward the data from the source node. In this case, n time slots are needed for n-hop forwarding. In addition, each relay node is only involved in one receiving and one transmitting. For the proposed protocol, the time slots cost is still n. However, for the relay node 2 to n−1, an extra transmitting is needed. Thus, the security comes from the trade-off of consuming of hardware and computational complexity of relay nodes.

The time slots cost of the cryptography approach is also n and relay node will only forward the encrypted data, but key negotiation is needed before the starting of the transmission. As previously mentioned, in WSN network, the key negotiation is still the hard problem, so it will definitely consuming much more hardware and computational complexity. Thus, we can conclude the proposed physical layer network coding protocol enjoys transmission efficiency than the cryptography approach. In addition, we will show the security level of these two approaches is identical.

4.3 Security Performance Analysis

We first discuss the security performance to against the untrusted relay. The relay tries to recover c_t with the decoded signal. There are three types of decoded signal for the relay nodes. One is for the first relay node R_1, one is for the last relay node R_{n-1} and another type is for all other relay nodes.

For relay node R_1, the decoded signal is $c_t \oplus c_2$. With the reason that R_1 has no information of the pseudorandom sequence c_2, this is analog to the stream cipher, *i.e.*, the relay will only obtain the sum of the data and the pseudorandom sequence severing as the key.

For the relay node R_i for $1 < i < n-1$, the decoded signal is $c_t \oplus c_i \oplus c_{i+1}$. However, by subtracting its self information, the situation will reduce to a sum of the data and a pseudorandom sequence. Thus, the security analysis is identical with the R_1.

For the relay node R_{n-1}, the decoded signal is $c_t \oplus c_{n-1} \oplus c_r$. By subtracting c_{n-1}, it is also a sum of the data and a pseudorandom sequence which is identical with the situation of R_1.

For the external eavesdroppers, we conclude they cannot launch stronger attack than the relay nodes with two reasons. First, the noise can be perfectly removed at the relay node, however, the noise is an important factor for the received signal at external eavesdroppers. Thus, the eavesdroppers will definitely get more errors when they try to recover c_t. Second, the summed signal after the first time slot will be the data c_t and another two pseudorandom sequences. The relay node can subtract its own pseudorandom sequence, however, the external eavesdroppers cannot subtract it. Thus, the data at the external eavesdroppers is hidden with two pseudorandom sequences leading the external eavesdroppers' attack is harder.

5. CONCLUSION

In this paper, we applied the physical layer network coding into wireless sensor network. We consider the situation that the source node will transmit its gathered data to the sink node with help of multiple relay nodes. Every three consecutive three nodes will form a multiple channel in which two side nodes align their signals at the middle node. By conducting physical layer network coding, the received signal at each relay is a summed of the data and a pseudorandom sequence. By doing so, the untrusted relays as well as external eavesdroppers cannot recover the data from the source node. Two types of physical layer network coding algorithms have been discussed including BPSK coding and nested lattice coding. The transmission and security performance are analyzed after the protocol introduced.

ACKNOWLEDGEMENT

This work is supported by: National Natural Science Foundation of China (No. 61101147), The National Basic Research Program of China (973 Program, No. 2012-CB316100), Specialized Research Fund for Doctoral Program of Higher Education (No. 20110203120004), Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2014JZ018), Science Research Plan in Shaanxi Province of China (No.

2013K06-15), The Fundamental of Research Funds for the Central Universities (No. K5051301006), The 111 Project (No. B08038), National Natural Science Foundation (No. 61472308), Science Research Plan in Shaanxi Province of China (No. 2016GY-085), the 111 Project (No. B16037).

REFERENCES

1. I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, Vol. 16, 2014, pp. 266-282.
2. C. T. Cheng, H. Leung, and P. Maupin, "A delay-aware network structure for wireless sensor networks with in-network data fusion," *IEEE Sensors Journal*, Vol. 13, 2013, pp. 1622-1631.
3. G. Ping, W. Jin, H. G. Xue, S. K. Chang, and J. U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *Journal of Internet Technology*, Vol. 15, 2014, pp. 929-935.
4. K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: A survey," *IEEE Transactions on Systems Man and Cybernetics Part C*, Vol. 42, 2012, pp. 1243-1256.
5. H. Lin and H. Üster, "Exact and heuristic algorithms for data-gathering cluster-based wireless sensor network design problem," *IEEE/ACM Transactions on Networking*, Vol. 22, 2014, pp. 903-916.
6. Q. Liu, G. Gong, Y. Wang, and H. Li, "A novel physical layer security scheme for MIMO two-way relay channels," in *Proceedings of IEEE Globecom Workshops*, 2015, pp. 1-6.
7. Z. Liu, H. Seo, J. Großschädl, and H. Kim, "Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes," *IEEE Transactions on Information Forensics and Security*, Vol. 11, 2016, pp. 1385-1397.
8. Z. Liu, H. Seo, X. Huang, and J. Großschädl, "Efficient implementation of ECDH key exchange for MSP430-based wireless sensor networks," in *Proceedings of ACM Symposium on Information*, *Computer and Communications Security*, 2015, pp. 145-153.
9. Z. Liu, H. Seo, and Q. Xu, "Performance evaluation of twisted Edwards-form elliptic curve cryptography for wireless sensor nodes," *Security and Communication Networks*, Vol. 8, 2015. pp. 3301-3310.
10. Z. Liu, E. Wenger, and J. Großschädl, "MoTE-ECC: Energy-scalable Elliptic curve cryptography for wireless sensor networks," *Applied Cryptography and Network Security*, Springer Verlag, 2014, pp. 361-379.
11. L. Lu and S. C. Liew, "Asynchronous physical-layer network coding," *IEEE Transactions on Wireless Communications*, Vol. 11, 2012, pp. 819-831.
12. J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Transactions on Signal Processing*, Vol. 62, 2014, pp. 2185-2199.
13. J. Shen, H. W. Tan, J. Wang, J. W. Wang, and S. Y. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of*

Internet Technology, Vol. 16, 2015, pp. 171-178.
14. S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure compute-and-forward in a bi-directional relay," *IEEE Transactions on Information Theory*, Vol. 61, 2015, pp. 2531-2556.
15. Z. Xia, X. Wang, X. Sun, and B. Wang, "Steganalysis of least significant bit matching using multi-order differences," *Security and Communication Networks*, Vol. 7, 2013, pp. 1283-1291.
16. S. Xie and Y. Wang, "Construction of tree network with limited delivery latency in homogeneous wireless sensor networks," *Wireless Personal Communications*, Vol. 78, 2014, pp. 231-246.
17. G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, 2012, pp. 184-197.

Qiao Liu (刘樵) received the B.S. degrees in Communications Engineering from Xidian University in 2011. He is currently pursuing the Ph.D. degree in Information Security from the School of Cyber Engineering, Xidian University. His research interests include wireless network security, physical layer security, and cooperative communication.

Yong Wang (王勇) is an Associate Professor in the School of Cyber Engineering at the Xidian University. He received his B.S. degree in Electronic Mechanics from Xidian University in 2001, and M.S. degree in Computer Science from Xidian University 2004. In 2009, he received his Ph.D. degree in Signal and Information Processing from Xidian University. His current work concerns adaptive antenna design and cooperative communication.

Wenjing Zhang (张文静) received her B.S. and M.S. degree in Information Security from Xidian University in 2011 and 2014. She is pursuing the Ph.D. degree in Information Security from the School of Cyber Engineering, Xidian University. Her research interests include big data security and privacy preservation.

Hui Li (李晖) received B.Sc. degree from Fudan University in 1990, M.Sc. and Ph.D. degrees from Xidian University in 1993 and 1998. In 2009, he was with Department of ECE, University of Waterloo as a Visiting Scholar. Since 2005, he has been the Professor in Xidian University, China. Now, he is the Executive Dean of School of Cyber Engineering and Dean of School of International Education. His research interests are in the areas of cryptography, wireless network security, cloud computing security, privacy preservation, and information theory. He has published over 160 papers in academic journals and conferences. He served as TPC co-chair of ISPEC 2009 and IAS 2009, general co-chair of E-Forensic 2010, ProvSec 2011 and ISC 2011, honorary chair of NSS 2014, ASIACCS 2016.