Compressed Sensing Applied to Wireless Sensor Networks Security

Jianxun Zhao
Zhongzhou University
Zheng zhou, China, 450044
zhaojianxun@yeah.net

Jihai Huang
Zhongzhou University
Zheng zhou, China, 450044
huangjihai@sina.com

***Abstract*—Secure communication in wireless sensor networks (WSNs) is a challenging problem due to the scale and resource limitations. This means that most existing security protocols such as cryptography are not applicable in WSNs. However, more recent researches argue that encryption based on compressed sensing (CS) has the inherent advantage for security. And a measurement matrix used for sensing is usually constructed by a secret key. But establishment and assignment of the secret key is very difficult for wireless scenarios. In this context, we propose a security scheme for WSNs, which allows two legitimate nodes to establish a common secret key by exploiting joint channel characteristics of wireless channel. These characteristics between any two nodes are unique, unpredictable and decor relating rapidly in space. The established keys can then be used to construct measurement matrix and reconstruction matrix for the two nodes respectively. For improving bit rate and agreement of secret keys, some methods are also proposed in the paper. Analysis and simulation results show that, our proposed scheme ensures a high level of security for WSNs and also has the advantage of low computability complexity.**

Keywords-Compressed Sensing, Joint Channel Characteristics, Key Generation, Wireless Sensor Networks

I. INTRODUCTION

Designing WSNs is a big challenge due to strict constraints and conditions posed by specific applications and environments, which include power consumption, node simplicity, node cost, low signal leakage and non-line-of-sight propagation, severe multi-path, etc [1]. Among all of them, security is becoming a major concern because of the wide security critical an application of WSNs. Securing WSNs has been researched frequently in recent years. A few existing surveys on security issues can be found [2], [3]. However, these articles follow a conventional cryptographic approach, which based on pre-distributed keys or public-key schemes assuming that there are perfect key generation and key management. Obviously, these methods, which need high energy consumption and memory resource, are not suitable to WSNs. Many literatures have addressed the problem, among which, in [4], an encryption idea by utilizing CS has been mentioned for the first time. But it has not been addressed in detail. In [5], the secrecy of CS is researched, whose result is that CS can provide a computational guarantee of secrecy. Adem Orsdemir and H. Oktay Altun [6] examine the security and robustness of the CS-based encryption method.

We note that the security of CS is based on its superiority in random projection, which means the measurement matrix(the mapping from analog signal to digital signal) of CS is changed randomly. But another problem encountered is the establishment and consultation of the random projection between transmitters and receivers. They are also at the heart of traditional cryptographic protocols. Furthermore, the nodes in WSNs have limited battery lifetime and low computational capability, which increase these challenges. Recently, there have been several research contributions that follow an alternative method to generate keys using wireless channels, which can be used to construct the measurement matrix. Shared secret key generation is an application benefited from the randomness of the wireless channels. Reciprocity and spatial time variations of wireless radio channel provide the advantages [7]. However, the radio channel is reciprocal, there are some causations destroying the characteristics, which include additive Gaussian noise, the discrepancy of transceiver hardware and measuring no simultaneously and so on. So [8] presents a novel methodology which allows robust secret.

key extracted from radio channel measurements by using fractional interpolation and LKT(Karhunen-Loeve transform). However, the method has high computational complexity because of statistical signal processing problem. We also proposed a novel secret key generation method in [9], by more than one channel characteristic to optimize jointly. The quantification of joint channel characteristics can increase the secret key rate. At the same time, the problem of secret key generation from channel characteristics is translated to the minimum error problem of vector quantization. And a unilateral adjustment mechanism of cells is used to reduce bad impact produced by non-simultaneous measurement and the error of channel estimation.

Reviewing above all, we are motivated to propose a novel security scheme for WSNs. Our approach unifies CS technique and the result of [9]. The security of the encryption approach relies on the fact that the measurement matrix, which has the function of compression data, is not known to an attacker. However, an attacker does not achieve the pseudorandom keys, which come from the unique joint channel properties of wireless channel between two legitimate nodes, to generate the measurement matrix. Our results indicate that the proposed scheme is very available.

This paper is organized as follows: In section II, we discuss system model. In section III, we provide a novel security scheme for WSNs based on the method of [9]. In

Published by Atlantis Press, Paris, France.

section IV the simulation result is shown and compared to the analytical one. Finally, we provide a short conclusion in section V.

II. COMPRESSED SENSING BASICS AND SECURITY SYSTEM MODEL

A. Compressed sensing basics

The work of Candes, Romberg, and Tao [10] and Donoho[11] show that if a signal has a sparse representation in one basis then it can be recovered from a small number of projections onto a second basis that is incoherent with the first. Let $x \in R^{m\times 1}$ be a vector as $x = \varphi\theta$, where $\theta = R^N$ has k non-zero entries (i.e., it is k-sparse), φ is a basis of x. And its linear measurement is $y = Ax$, where $A \in R^{m\times n}$ is a transformation matrix. The transformation matrix has fewer rows than columns, i.e., $m < n$. y is obtained by mapping the vector x onto a basis that is incoherent with φ. Roughly speaking, incoherence means that no basis vector in φ has a sparse representation in the basis specified by A. This system of equations has infinite many solutions. For recovering x, an optimization problem can be cast as:

$$\min_x \|x\|_0 \text{ subject to } y = Ax \tag{1}$$

Where $\|x\|_0$ is the support of x. This problem is a non-convex optimization problem and a solution requires an exhaustive search over the solution space. However, the problem can be solved by greedy algorithms such as basis pursuit[12] and orthogonal matching pursuit[13], which are not guaranteed to achieve the optimum.

If the matrix A satisfies the restricted isometric property (RIP), that is

$$(1-\delta s)\frac{k}{n}\|x\|_2^2 \le \|Ax\|_2^2 \le (1+\delta s)\frac{k}{n}\|x\|_2^2 \tag{2}$$

Where δs is a sufficient small values, (1) can be alternated by[14]

$$\min_x \|x\|_1 \text{ subject to } y = Ax \tag{3}$$

Where $\|x\|_1$ denotes the ℓ_1 norm of vector x. In the presence of noise on measurements, we can get that $y = Ax + n$, where n denotes the noise vector. A similar problem can be denoted as [15]:

$$\min_x \|x\|_1 \text{ subject to } \begin{matrix} P(Y=0 \mid X=0) \neq P(Y=0)\,6.73\times 10^{-8} \\ I(X;Y) = 0 Ax = 0 y = 0 P(Y=0) < 1 \\ K = 0.1NM = 8KN \end{matrix} \tag{4}$$

Where δ represents the expected noise power in the observations. This formation provides a stable recovery of original signal value in the presence of noise.

B. System models

We also borrow from the conventional terminology of the security community by using three different parties: Alice, Bob and Eve. The three entities may be thought as wireless transmitters/receivers that are potentially located in separated positions. In our system model we assume that the eavesdropper Eve knows all of assumption between legitimate nodes Alice and Bob. She can also achieve both the channels between herself and Alice and Bob at the same time when Alice and Bob measure the channel between themselves for key generation. The only thing, Eve can not know, is the wireless channel characteristics between Alice and Bob because that she can not be very close to either Alice or Bob while they are generating their cryptographic keys. Literature [16] [17] addressed that the distance of more than a few multiples of the wavelength of radio waves being used will ensure that Eve achieve a different, uncorrelated radio channel. The model of proposed security scheme as shown in Fig.1.

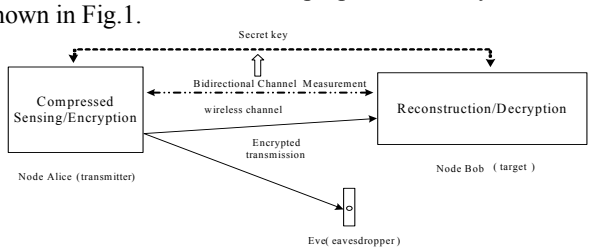

Figure 1. Flow diagram of the novel security scheme

We consider the scenario where two legitimate nodes Alice and Bob wish to establish a secure communication link in the presence of an unknown eavesdropper Eve. In establishing step, we consider that Alice and Bob each probe the common SISO (Single Input, Single Output) channel, which means that every node has only one antenna. Suppose two nodes, Alice and Bob, observe L channel characteristics (Amplitude, Phase and so on) $\tilde{h}_A$ and $\tilde{h}_B$ respectively, which are denoted by $\tilde{h}_A = [\tilde{h}_{A,1}, \cdots \tilde{h}_{A,2}, \cdots \tilde{h}_{A,L}]$ and $\tilde{h}_B = [\tilde{h}_{B,1}, \cdots \tilde{h}_{B,2}, \cdots \tilde{h}_{B,L}]$. Suppose there are C independent and identically distributed (i.i.d.) channel, which are the different time observations of the SISO channel. So define a matrix $\tilde{H}$ whose size is $L\times C$, as the measures of channel by Alice or Bob. So (5) can be achieved by bidirectional channel measurement

$$\begin{aligned} \tilde{H}_A &= \tilde{H} + \Delta\tilde{H}_A \\ \tilde{H}_B &= \tilde{H} + \Delta\tilde{H}_B \end{aligned} \tag{5}$$

Where $\Delta\tilde{H}_A$ and $\Delta\tilde{H}_B$ is estimate error of Alice and Bob severally, which affected by measurement, noise and so on. So the measurement matrix A can be written as

$$A = M\left(Q(\tilde{H})\right) \tag{6}$$

Where $M(\cdot)$ is the operation of converting a vector to a matrix. And $Q(\cdot)$ is the operation, which quantizes the channel matrix as a vector. Supposing that original signal vector x is a sparse signal. Then the signal received by Bob and Eve are completely different:

$$\begin{aligned} Y_B &= H_{AB}Ax + N_{AB} = H_{AB}M\left(Q(\tilde{H}_A)\right)x + N_{AB} \\ Y_E &= H_{AE}Ax + N_{AE} = H_{AE}M\left(Q(\tilde{H}_A)\right)x + N_{AE} \end{aligned} \tag{7}$$

Where H_{AB} and H_{AE} denote the channels between Alice & Bob and between Alice & Eve, respectively, N_{AB} and N_{AE} is the noise added at Bob and Eve. Although Eve can achieve H_{AE} through receiving the probe signal of Alice, she

can not know the matrix $\tilde{H}_A$. That is to say, she can not achieve reconstruction matrix for recovering the original signal.

III. NOVEL SECURITY SCHEME FOR WSNS

In this section, we introduce the encryption concept based on CS and key generation using the wireless channels. Conventionally, signals are sampled conforming to the NY Quist sampling rule. Then sampled data is compressed to reduce the data and encrypted for security. The encrypted data then go through a channel and is decrypted by the intended user. Both the two communicators share a secret key. However, compressed sensing unifies the sampling, compression and encryption steps to one step. Then the receiver can recover the original signal with the knowledge of matrix. This encryption comes naturally and requires no additional cost. The only problem, which blocks the existing encryption, is distribution of security keys. In this paper, we generate security keys by using the characteristics of wireless channels as [9]. The established keys can then be used to construct measurement matrix and reconstruction matrix for the two nodes respectively.

Analysis of Key Generation Protocol of [9]

In [9], we present a key generation protocol which is suitable even limited volume and power by using joint process, which can achieve high secret key rate and consistency.

Upper Bound of Secret Rates: According to expatiation above, Alice and Bob can achieve the vectors $\tilde{h}_A$ and $\tilde{h}_B$, which correlates to real channel characteristics $\tilde{h}$. That is to say, $\tilde{h}_A$ and $\tilde{h}_B$ are statistic similar because they originate from the same source. Alice and Bob wish to generate a common secret key K, based on their estimation of the channel characteristics vectors. Note that $H_A(K)=H_B(K)$, J_A and J_B are the output of quantization and encode. Suppose that the key disagreement probability satisfies

$$P(J_A \neq J_B)=\xi \tag{8}$$

for a small nonnegative number ξ. According to Fano's Lemma [18], there have been

$$H(J_A \mid J_B) \le h_0(\xi)+\xi \log_2(|S|-1) \tag{9}$$

Where $h_0(\xi)=-\xi\log_2\xi-(1-\xi)\log_2(1-\xi)$, $|S|$ represents the number of distinct values J_a takes on with nonzero probability. This equation shows that if $\xi \to 0$, then $H(J_a \mid J_b) \to 0$. So $H(J_a) \le I(K_a,K_b)+H(J_a \mid J_b)$. Note that K_a and K_b are respectively the quantized versions of $\tilde{h}_A$ and $\tilde{h}_B$, so we have $I(K_a,K_b) \le I(\tilde{h}_A,\tilde{h}_B)$. That is to say, if the key disagreement is negligible which implies $H(J_a \mid J_b) \to 0$. The entropy rate of the resulting secret key $H(K)$ is upper bounded by mutual information $I(\tilde{h}_A;\tilde{h}_B)$.

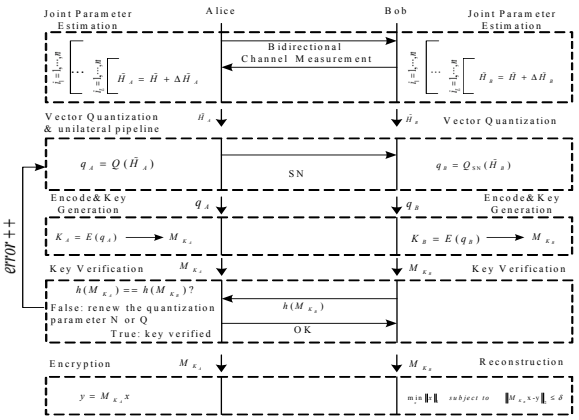

Figure 2. CS-based secrecy Protocol

CS-based secrecy Protocol and Security Analysis

Fig.1 illustrates the security model in the paper. Compressed sensing unites the sampling, compression, and encryption steps for Alice. And the transform matrix is formed by using security key, which comes from wireless channel characteristics between Alice and Bob. The characteristics belong to Alice and Bob only. So the linear measurement matrix is available to the node Bob in order to recover the original signal. Without the knowledge of the received signal appear encrypted to anyone eavesdropping on channel. The complete protocol of CS-based WSNs security is shown in Figure 2.

The proposed secrecy protocol for WSNs operates in five phases. In the joint parameter estimation, the channel characters are acquired by bidirectional channel measurement, which due to the reciprocity of wireless channel state information strongly correlated measurements are collected by Alice and Bob. In the vector quantization & unilateral pipeline, some steps are used for agreement between the two legitimate parties. In the encode & key generation, the output of vector quantization is encoded and the result is used to form measurement or reconstruction matrix. Then the key verification phase ensures correct key agreement. In this paper, we assume that information reconciliation will be part of the system design, but we do not explore its use. We want to reduce the quantity of information reconciliation that must be performed in order to agree on a shared secret matrix by minimizing the rate of bit disagreement reliably. The encryption phase encrypts the input signal x to achieve y. Then Bob reconstructs the original signal by solving a convex optimization problem with reconstruction matrix.

Information theoretical secrecy based on the statistical properties of a system provides protection even in the face of a computational unbounded adversary. For our scheme, if the conditioned probability of a message is equal to the priori probability of the message, $P(X=x \mid Y=Ax)=P(X=x)$. Alternatively, this condition can be stated as $I(X;Y)=0$. However, since A is linear, $x=0$ implies that $y=0$ Therefore $P(Y=0 \mid X=0)=1$. If $P(X=0)<1$ and we can conclude

that $P(Y=0)<1$. Therefore $P(Y=0 \mid X=0) \neq P(Y=0)$ that is to say X and Y are statistically dependent. So the scheme proposed does not achieve information theoretical secrecy. But compressed sensing can provide computational secrecy [5], so the computational cost of reconstructing the signal is high. Eve can only accompany with a random search, which is too expensive.

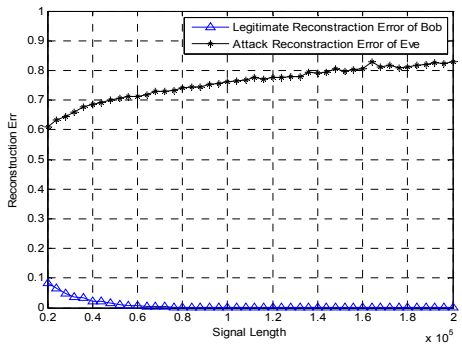

Figure 3. Compare Reconstruction Error of Bob to Attack Reconstruction Error of Eve

IV. Simulation Results

In this section, for evaluating the security our work, we use the security key generated above to form the measurement matrix for Alice and reconstruction matrix for Bob. For Eve we generate some stochastic matrices to reconstruct the initial signals sent by Alice. The initial signals are spike, consisting zeros except for spikes of magnitude one. The number of spikes is $K=0.1N$ and the number of measurement is $M=8K$. For each message length N, Fig.3 shows the result of attacks originating by Eve. From the graph, it is apparent that Eve experiences reconstruction error that increases with N. At the same time, Bob reconstructs with low error. For example, for $N=60000$ the average reconstruction error is 6.73×10^{-8} with the security key generated in [9].

V. Conclusion

Security in WSNs is a new area of research. It is worth studying for its linchpin in some applications. This paper has discussed the security of WSNs. A novel security scheme based on CS and wireless channel secret key is presented. By relying on wireless channel characteristics, security key is extracted, which is used to form the measurement and reconstruction matrix for CS. After providing a discussion of security protocol and security, some simulations are done. Results of simulation indicate that the proposed scheme can solve the problem WSNs is encountering, which has certain academic sense and practical value.

References

[1] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys Tutorials, vol. 11. no.2, second quarter 2009, pp.52-72

[2] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2-28, 2005.

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in WSNs," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2-23, 2006.

[4] D. Takhar, J. N. Laska, M. B. Wakin, M. F. Duarte, D. B. S. Sarvotham, K. F.Kelly, and R. G. Baraniuk, "A new camera architecture based on optical-domain compression," in Proc. IST/SPIE Symposium on Electronic Imaging: Computational Imaging, vol. 6065, 2006, pp. 129-132.

[5] Yaron Rachlin and Dror Baron, "The Secrecy of Compressed Sensing Measurements"

[6] Adem Orsdemir, H. Oktay Altun, Gaurav Sharma, Mark F. Bocko," On the Security and Robustness of Encryption via Compressed Sensing" Military Communications Conference, 2008, Milcom 2008,IEEE pp.1-7.

[7] Neal Patwari, Jessica Croft, Suman Jana, and Sneha Kumar Kasera HighRate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements, IEEE Transactions on Mobile Computing ,Vol.9, No.1, January 2010 pp. 17-30.

[8] Jessica Croft, Neal Patwari, Sneha K. Kasera, Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors, IEEE 2010, pp,70-81

[9] W. Y. Luo, L. Jin, B. P. Zhou, Shared Secret Key Generation from Joint Wireless Channel Characteristic, Acta Electronica Sinica, china, accepted.

[10] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles:Exact signal reconstruction from highly incomplete frequency information," IEEE Transactions on Information Theory, vol. 52(2), pp. 489-509, 2006.

[11] D. Donoho, "Compressed sensing," IEEE Transactions on Information Theory, vol. 52(4), pp. 1289-1306, 2006.

[12] Chen S B, Donoho D L, Saunders M A. Atomic decomposition by basis pursuit. SIAM Journal on Scientific Computing, 1998, 20(1): 33-61

[13] Tropp J, Gilbert A. Signal recovery from random matching pursuit. Transactions on Information Theory, measurements via orthogonal 2007, 53(12): 4655-4666

[14] E. Candes and T. Tao, "Decoding by linear programming," IEEE Trans. Inform. Theory, vol. 51, no. 12, Dec 2005.36-41

[15] E. Candes, J. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," Comm. Pure Appl. Math., vol. 59, no. 8, pp. 1207-1223, Aug 2006.

[16] S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In ACM MOBICOM Conference, Sept. 2008.pp 698-721

[17] G. D. Durgin. Space-Time Wireless Channels. Prentice Hall PTR, 2002.

[18] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik, "Radio-telepathy: Extracting a Secret Keyfrom an Unauthenticated Wireless Channel," to appear in ACM Mobicom 2008, Sept,pp 58-66