International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

ENHANCING THE LIFE TIME OF WIRELESS SENSOR NETWORK USING LITE-IDE

N.Dhivya,
Research Scholar,
Department Of Computer Science,
Theivanai Ammal College for Women,
Villupuram,Tamilnadu,India.

Dr.R.Suguna,
Head,
Department Of Computer Science,
Theivanai Ammal College for Women,
Villupuram,Tamilnadu,India.

Abstract - Wireless sensor networks (WSNs) provide a flexible way to detect spatial information through a large number of sensor nodes. This paper considers energy efficient distributed data gathering methods for correlated data field monitoring in multi-hop wireless sensor networks (WSNs) via Lite-IDE based hierarchical node authentication protocol. The proposed protocol is to solve problem of energy imbalance. The proposed method is Lite-IDE based authentication scheme is proposed for node authentication, which needs to exchange the authentication messages, and key generation. We provided complexity and energy cost analysis of our protocols and show that our protocols are more energy efficient and suitable for WSN.

Keyword : Data gathering, Key generation, Energy dissipation.

I. INTRODUCTION

Sensor networks feature low-cost sensor devices with wireless network capability, limited transmit power, resource constraints and limited battery energy. The usage of cheap and tiny wireless sensors will allow very large networks to be deployed at a feasible cost to provide a bridge between information systems and the physical world. Wireless sensor network (WSN) applications are growing. While the importance of security, it is still largely ignored since the problem is considered impractical to solve given the limited computation and energy resources available at node level. Recent advices in wireless communication and electronics have enable the development of low-cost, low power, multifunctional sink nodes that are small in size and communicate in short distances, which are capable of sensing, data processing, and communicating. In LEACH based protocol(IE-LEACH, IL-LEACH), data encryption mechanism LEACH based protocol is proposed, In AM-E, when BS(base station) generates authentication key, it uses ID and residual energy of sink node. Therefore, in order to securely transmit data in WSN networks, a Lite-IDE-based hierarchical node authentication protocol is proposed in our paper. This paper solved the problem that too much energy is consumed during the generation of authentication key because sink node directly communicates with BS. This proposed paper uses logical hierarchical structure for nodes authentication. All nodes are divided with logical clustering structure. After authentication, base station distribute session key to cluster header, then each sink nodes receives the group key through cluster header. By using group key and session key mechanisms, the experiment result showed that the energy consumption in first round is reduced about 34% and the total energy consumption with 1000 joined nodes in the entire lifetime is reduced about 29%.

II. RELATED WORKS

The problem of data gathering and compression using CS is widely developed in the literature. Even though a lot of attention is paid to reconstruction algorithms and mathematical aspects, practical aspects and implementation problems have been gaining a lot of interest lately. The general problem of using CS in WSNs is investigated in several works, like in [13], where the authors analyze synthetic and real signals against several common transformations to evaluate the reconstruction performance, or in [14], where the measurement matrix is created jointly with routing, trying to preserve a good reconstruction quality. Furthermore, in [15], the authors improve reconstruction by reordering input data to achieve a better compressibility. In general, all of these papers address the problem of the signal reconstruction, but they lack a real consideration about energy involved in compression. When real hardware is considered, considerations about CS have to be revised. One of the first papers trying to address the problem of energy consumption for compression dealing with the problem to generate a good measurement matrix using as low energy as possible is [3]. In this work, the research is focused on wireless body sensor networks (WBAN) for real-time energy-efficient ECG compression. Other works that focus on bio-signals and WBANs are [16,17]. This is a quite different research field with respect to WSNs, where the presence on several nodes sensing the same environment permits one to exploit the distributed nature of the signals to improve the quality of recovery. However, CS is today applied in several other signal processing fields, from video compression [2] to underwater acoustic OFDMtransmission [18] and to air quality monitoring [19].

In fact, several works, like [20] or [21], deal with the use of CS when multiple nodes are used in a joint reconstruction. The best known technique used to exploit the existing correlation among several nodes in a WSN is distributed compressed sensing (DCS) [9,10], which permits new distributed coding algorithms for multi-signal ensembles that exploit both intra- and inter-signal correlation structures. Besides the classical digital implementation of CS used in all of the aforementioned papers, in this paper, we deal also with CS when the signals are sampled at a sub-Nyquist frequency. Usually, in the literature, this compression technique is referred to with the name of analog CS. This is because, usually, the subsampling is

performed at the ADClevel, dropping samples during the acquisition and analog-to-digital conversion stage. For example, in [22], the effects of circuit imperfections in the analog compressive sensing architectures are discussed.

While it is common in the literature to find papers like the two aforementioned addressing the problem of analog CS with a focus on the hardware called analog-to-information converters (AICs), other works investigate the problem from a higher system-level prospective when the samples are not discarded by the ADC architecture, but by the device performing the sensing. One of the papers dealing with this specific case is [23], where the analysis on energy consumption is totally neglected, and it is strictly related to the specific application of the pulse oximeter. Differently from environmental signals, the signals obtained by the oximeter present a much higher temporal correlation, presenting small variations in its temporal evolution.In [26], the authors use a weighted form of the basis pursuit to reconstruct signals gathered using a sparse measurement matrix addressing also the problem of the energy spent in generating the random projection matrix on the node itself. Nevertheless, the aim of the paper is quite different from ours: the authors in [26] want to detect a specific event characterized by a well-defined frequency, and this makes it easier to train the reconstruction algorithm to detect the specified event; whereas in our approach, we address the reconstruction without any priors about the signal to recover and using temporal or spatial correlation as data training for reconstruction.

III. SYSTEM ANALYSIS

System analysis is the act, process, or profession of studying an activity typically by mathematical means in order to define its goals or purposes and to discover operations and procedures for accomplishing them most efficiently.

Existing System : Wireless sensor networks (WSNs) consisting of densely deployed battery-powered sensor nodes have been proposed for different kinds of measuring purposes, such as monitoring light, temperature or humidity. There are three main challenges in WSNs, i.e., lifetime, computational ability and bandwidth constraints. CS framework motivated by the asymmetrical structure of WSNs CS, also called compressed sensing or Sub-Nyquist sampling, has a surprising property that one can recover sparse signals from far fewer samples than is predicted by the Nyquist-Shannon sampling theorem. CS trades-off an increase in the computational complexity of post-processing against the convenience of a smaller quantity of data acquisition and lower demands on the computational capability of the sensor node.

Problem Definition

1. Some of the samples are lost during the transmission
2. RQI trend has a floor effect owing to the sampling noise in the samples reserved for comparison, which cannot be computed or estimated.
3. Computational complexity is increased

Proposed System: Improving lifetime is directly related to Energy efficiency which is the most required quality in a sensor network where each node consumes some energy with each transmission over the network. The proposed work defined the same direction to improve the network life. This work is about to perform the energy effective routing so that the network life and network throughput will be improved. we proposed an Lite-IDE-based hierarchical node authentication model. BS serves as the CA(certification center) of first level to authenticate all cluster headers. In our proposed model, cluster header operates as the medium between authentications of BS and nodes for authentication.

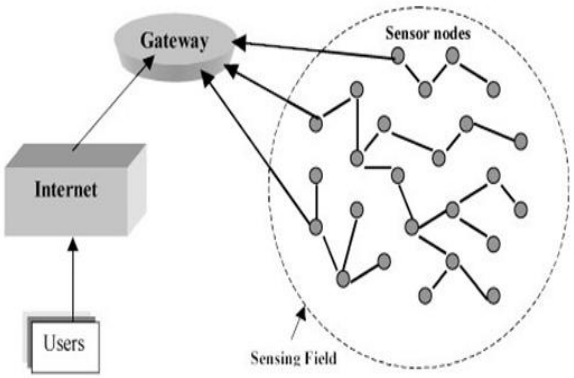

Fig: ***Wireless Sensor Network***

This model consists of base station who acts as CA, cluster header who acts as sub-CA (sCA) and member nodes that join to cluster header. Cluster header is authorized a sCA after being authenticated by BS. Furthermore the security among cluster headers can be guaranteed without multi-hop mutual authentication between cluster headers. Member node is authenticated finally by BS through cluster header as the medium. BS notifies the cluster header that this member node is an attacker and then cluster header broadcasts ID of the attacker to all nodes to avoid communication with it.

Advantages

1. Energy Consumption is achieved
2. Security is achieved
3. Improved performance
4. Message replay attack is overcomes
5. Network lifetime is increased

IV. LITE-IDE METHOD

Step 1: *Authentication Request Phase*

Cluster header sends AREQ message to BS for authentication requesting. The message includes: ID of cluster header, seed value N1, private information value encrypted by message (CH) and random value none to avoid message reply.

$$CH \rightarrow BS: AREQ\{N1, ID_{CH}, E_{ID_{CH}}(ID_{CH} \| \delta_{CH} \| none)\}$$

Step 2: *Validation and Search*

The BS authenticates cluster header with the message received from cluster header. BS transmits authentication request message to authentication DB server using searchquery, and DB searches the Key Pair (ID, password) of cluster header. If the ID exists, the sent cluster header is valid. The authentication DB sends a repVerify message to BS which includes the private information of the requested node.

$$BS \rightarrow DB: reqSearch(ID_{CH}, PW_{CH})$$
$$if\ match \quad DB \rightarrow BS: repVerify(ID_{CH}, \delta_{CH}, PW_{CH})$$
$$if\ notmatch \quad BC^{*}: EM(0, ID_{CH})$$

Step 3: *Session Key Generation*

BS receives the repVerify message from DB and generates session key based repVerify message (CH). Session key is generated by do the hash function to ID of cluster header (IDCH), password of cluster header (PWCH), private value (CH) and random number (none) and then sent to cluster header with a authentication response message.

$$BS: \alpha_{CH} = H(ID_{CH_i} \oplus PW_{CH_i} \oplus \delta_{CH} \oplus none)$$

$$BS \rightarrow CH: AREP\{N2, E_{ID_{CH}}(ID_{CH} \| \alpha_{CH} \| none)\}$$

In the above (step1) to (step 3), Lite-IDE-based message is transmit. Cluster header gets authenticated by BS and is assigned a session key for secure communication between cluster headers. Every time when cluster header is changed, the session key needs to be updated.

V. PERFORMANCE EVALUTION

To analyze the energy efficiency of the proposed protocol, energy consumption for authentication key establishment in member node and cluster header is respectively defined in equation (2) and equation (3). Equation (2) is the energy consumption in cluster header, while equation (3) is the energy consumption in member node.

$$AE_{CH} = T\left[(2\delta + \mu R^k)\left(\frac{d^2}{R^2 - 1}\right) + \left(1 + \mu R^2\right)\right] \quad (2)$$

Equation (3) is the energy consumption which is needed in the multi-hop communication of cluster header.

$$AE_{MN} = T(\delta + \mu d^k) \quad (3)$$

Based on equation (2) and equation (3), equation (4) is the whole energy consumption for authentication key establishment in a cluster.

$$AE_{cluster} = \sum_{i=1}^{r} AE_{CH} + AE_{MN} \quad (4)$$

In the next, we calculated the energy consumption for message communication using the authentication key. In a round, the whole energy consumption for communication in a cluster can be calculated as in equation (5), whereas the energy consumption in member node for the communication is defined in equation (6).

$$E_{CH} = M \times E_{elec}\left(\frac{n}{k} - 1\right) + M \times \frac{n}{k} + M \times e_{fs} {d_{BS}}^2 \quad (5)$$

$$E_{MNs} = M \times E_{elec} + M \times e_{fs} \times {d_{CH}}^2 \quad (6)$$

Summarizing the above equations form (2) to (6), we can calculate the whole energy consumption in a round, which includes the energy consumption for key establishment and for message communication, in both cluster header and member node. The result is calculated as equation (7):

$$E_{tot} = M\left\{2nE_{elec} + nE_{DA} + e_{fs}\left(k{d_{BS}}^2 + n{d_{CH}}^2\right)\right\} \quad (7)$$

In our simulation, energy consumption for authentication key establishment is calculated based on the energy consumption in cluster header equation (2) and the energy consumption in member nodes equation (3) in one round. Furthermore, we analyzed the energy consumption equation (5), (6) in communications for authentication key between cluster header and member node and the energy consumption within the cluster equation (7). Fig. 1 shows the energy consumption of all participated nodes for authentication in different rounds. Our protocol is like LEACH based protocol that initial few round. But while continuous round our protocol energy consumption less then LEACH based protocol.

VI. CONCLUSION

In this paper, we proposed a Lite-IDE-based hierarchical node authentication mechanism for secure data transmission in WSN. In these mechanisms, AREQ/AREP message for node authentication consume much energy and the direct communications between BS and cluster header nodes also need much energy, this causes large burden for nodes have very limited energy. And it also influents the essential works of nodes, it is data sense and collection. Furthermore, because only authenticated nodes can participate in the communication, the security of data is assured.

VII.REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393–422, 2002.

[2] D. Donoho, "Compressed sensing," Information Theory, IEEE Transactions on, vol. 52, no. 4, pp. 1289–1306, 2006.

[3] R. Baraniuk, "Compressive sensing," Signal Processing Magazine, IEEE, vol. 24, no. 4, pp. 118–121, 2007.

[4] E. Candes and M. Wakin, "An introduction to compressive sampling," Signal Processing Magazine, IEEE, vol. 25, no. 2, pp.21–30, 2008.

[5] J. Haupt, W. Bajwa, M. Rabbat, and R. Nowak, "Compressed sensing for networked data," Signal Processing Magazine, IEEE,vol. 25, no. 2, pp. 92–101, 2008.

[6] X. Qu, X. Cao, D. Guo, C. Hu, and Z. Chen, "Combined sparsifying transforms for compressed sensing mri," Electronics Letters,vol. 46, no. 2, pp. 121–123, 2010.

[7] O. Michailovich, Y. Rathi, and S. Dolui, "Spatially regularized compressed sensing for high angular resolution diffusion imaging," Medical Imaging, IEEE Transactions on, vol. 30, no. 5, pp. 1100 –1115, May 2011.

[8] Y. Lin, B. Zhang, W. Hong, and Y. Wu, "Along-track interferometric sar imaging based on distributed compressed sensing,"Electronics Letters, vol. 46, no. 12, pp. 858–860, 2010.

[9] Y. Liu, M. Wu, and S. Wu, "Fast omp algorithm for 2d angle estimation in mimo radar," Electronics Letters, vol. 46, no. 6, pp.444–445, 2010.

[10] Y. Yu, A. Petropulu, and H. Poor, "Measurement matrix design for compressive sensing based mimo radar," Signal Processing, IEEE Transactions on, vol. PP, no. 99, p. 1, 2011.