http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (7): 1361-1368, 2010
ISSN 1812-5638

CADS: Co-operative Anti-fraud Data Storage Scheme for Unattended Wireless Sensor Networks

Zhiqiang Ruan, Xingming Sun, Wei Liang, Decai Sun and Zhihua Xia
School of Computer and Communication, Hunan University,
No. 252, Lushan South Road, Changsha, 410082, China

Abstract: In this study, we focus on design efficient security techniques to maximize chances of data survival in wireless sensor networks, which involve disconnected or unattended operation with periodic visited by the sink, we refer to such networks as UWSNs. Data security in such UWSNs poses a number of challenges when applied in security-sensitive environments. First, sensors must accumulate data for a long time until it can be off loaded to a periodic sink. The adversary has lots of time to mount various attacks that aim to learn, erase, or modify potentially valuable data collected and held by sensors. Second, there is no ever-present sink, thus real time detection dose not help and the adversary can reach its goal and remain undetected. To address these security problems, we present CADS, a novel Co-operative and Anti-fraud Data Storage scheme for UWSNs by integrating the techniques of secret sharing and Discrete Logarithm Problem (DLP). We first propose a share generation and distributed scheme to achieve reliable and fault-tolerant initial data storage by providing redundancy for original data components, we then utilize discrete logarithm problem to ensure the integrity of the distributed data shares. The proposed scheme enables individual sensors to verify all the related data shares simultaneously in the absence of the original data in each round. Security analysis and simulations show that the proposed scheme has resistance against node capture attacks and outperforms existing security scheme in terms of data survival quantity and false negative probability.

Key words: Wireless sensor network, security, secret sharing, discrete logarithm problem, integrity

INTRODUCTION

Wireless Sensor Networks (WSNs) are envisioned to be extremely useful for a broad spectrum of emerging civil and military applications (Akyildiz *et al*., 2002), such as remote surveillance, habitat monitoring and collaborative target tracking. Security issues have received a lot of attention within the last decade. In particular, previous research on wireless sensor networks has been focused on key management (Chan *et al*., 2003; Yu and Guan, 2008), secure routing protocol (Kariof and Wagner, 2003; Bairaktaris *et al*., 2008; Meng *et al*., 2008), countermeasure against various attacks (Raymond and Midkiff, 2008) (Madria and Jin, 2009), energy efficient scheme (Wei *et al*., 2007) and so on. In these WSN security issues, data collection is performed in, or near, real time, that is, a trusted collector (such as a sink) is assumed always present. Presence of an online sink enables nodes to submit measurements soon after sensing. Consequently, if there existing node capture activities, the sink can take appropriate action immediately to prevent further compromise, thus an adversary capable of compromising nodes and corrupting data has relatively little time to attack.

Although, most of WSNs operate in this mode, there are WSNs scenarios and applications that do not fit into the real-time data collection model (Kamra *et al*., 2006) (Benenson *et al*., 2007). We refer to such networks as Unattended WSNs or UWSNs, for example, a tree-mounted WSN composed of noise sensors, installed in a protected area to monitor firearm discharge to detect poaching or sawing to detect illegal tree logging. The size of the protected area, its inaccessibility and/or the difficulty of hiding a sink, can motivate the requirement for an itinerant sink. We further narrow the scope to UWSNs operating in hostile environments. Such as, a subterranean sensor network aimed at monitoring sound and vibration produced by troop movements (or border crossings). One common feature in these examples is that constant physical access to the entire network is impossible and sink visits are discontinuous. Consequently, sensors cannot off load data in real time, they must accumulate data in situ and wait for some external trigger or an explicit request by the sink.

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, No. 252, Lushan South Road, Changsha, 410082, China Tel: 86-731-8821341 Fax: 86-731-8821780

Unattended sensors deployed in such environments represent an attractive and easy target for an adversary. The inability of the sensors to off load data promptly exposes them and their data to increase risk. Without external connectivity, sensors can be compromised and collected data can be read, altered, or simply erased. Sensor compromise is a realistic threat because a typical sensor is a mass-produced commodity device with no specialized secure hardware or tamper-resistant components (Kahn *et al*., 1999). The adversary can compromise a maximum number of sensors within a particular interval. This interval can be much shorter than the time between successive visits of the sink. Given a sufficient number of intervals, the adversary can subvert the entire network.

Therefore, the greatest challenge is to ensure data survival for long enough that it can be collected by the itinerant sink. A few related works (Pietro *et al*., 2008a, b; Pietro *et al*., 2009a) regarding unattended wireless sensor networks can be found in the literature, but none of them satisfies the overall requirements of data confidentiality, dependability, integrity and efficiency.

In this study, we propose CADS, a novel Co-operative and Anti-fraud data storage scheme for UWSNs by integrating the techniques of secret sharing and discrete logarithm problem. In our scheme, the data-originating sensor partitions the original data into multiple shares based on the enhanced secret sharing techniques. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based techniques (Hara and Madria, 2006) and achieves reliable data storage by providing redundancy for original data components. To ensure data integrity and availability, we utilize Discrete Logarithm Problem (DLP) (Konoma *et al*., 2005), which allows the share holders to perform dynamic data integrity checks in a random way with minimum overhead. Since, the data-originating sensor appends distinct authentication information to each data share, all share holders can verify the distributed data shares independently in each check.

This study makes two main contributions. First, the data survival rate is significant improved and the false negative probability can be reduced to almost zero, thus any unauthorized modifications can be detected in one verification operation. Second, our scheme can verify the integrity of aggregated data shares with great efficiency. We show through security analysis and simulation that our scheme is highly effective and efficient and can be well suited for resource-constrained WSNs.

MODELS AND ASSUMPTIONS

Network models: As shown in Fig. 1, we envision a wireless sensor network composed of a sink which is a trusted party and the two-tier architecture which comprising of a large number of resource-poor sensor nodes at the lower tier and the upper tier contains fewer relatively resource-rich master nodes. The network region is partitioned into physical cells (or grids), each containing a master node in charge of sensor nodes in that cell. Sensor nodes are mainly responsible for sensing tasks, while master nodes collect data from sensor nodes and answer the queries from the network owner. Master nodes perform more resource-demanding computation, communication and storage tasks. To prevent storage overflow of master nodes, mobile sinks can periodically dispatched to collect data and empty the storage of master nodes.

The reliance on master nodes for data storage and query processing raises serious security concerns. In particular, many target application environments similar to UWSNs. Master nodes are attractive targets of attack and might be compromised by the adversary. Recent works (Mache *et al*., 2008; Du *et al*., 2009) studied Heterogeneous Sensor Networks (HSNs), where master nodes equipped with tamper-resistant hardware. Besides, the rapid progress in new-generation sensor nodes with significant storage technology makes it possible to equip each of the relatively fewer master nodes with several gigabytes of NAND flash storage. In addition, the number of master nodes in such heterogeneity is small (e.g., 20 master sensors and 1000 sensor nodes in UWSNs). Hence, the total cost of master nodes in UWSNs is low. As this study represents the very first attempt to develop data storage protect for UWSNs, thus we assume that the master nodes are equipped with such technology. It may remain economically prohibitive to furnish each sensor node with tamper-proof hardware and large flash storage.

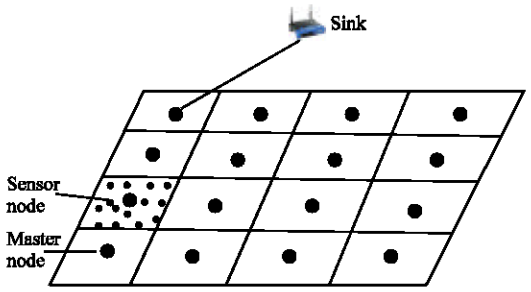

Fig. 1: Two tiered networks

Adversary models: We consider a powerful adversary, hereafter referred to as an μADV. One important feature that separates it from other adversarial models is its mobility. We assume that an μADV can compromise a subset (up to a certain size) of sensors within a given time interval. The time it takes an μADV to compromise a set of nodes is much shorter than the time between two successive visits of the sink. Thus, given enough compromise intervals, an μADV can gradually subvert the entire network. Once an μADV occupies a given node, it can be read, altered, or simply erased to the storage, memory and all of the communication interfaces of the node. At the very least, it can learn all node secrets, as well as eavesdrop on all relevant communication. Specifically, the adversary has one central goal: to prevent certain data collected by sensors from ever reaching the sink.

Of course, nothing prevents an μADV from physically destroying or damaging sensors, in particular because the network is unattended most of the time. However, such crude behaviours leave evidence. We tend to assume that an μADV is subtle and prefers to operate in a stealthy manner. Therefore, because it wants to leave no trail, the movements of an μADV are unpredictable and they are untraceable. Note that if the adversary compromises a sensor node and resides there, it can always respond the verifier with the correct data and successfully pass the periodic data integrity checks. In fact, there is no way to detect such a compromised sensor if it is controlled by the adversary and behaves properly all the time.

For lack of space, we follow the adversary model in (Pietro *et al*., 2009b) and focus on dealing with compromised general sensor nodes in this study. The investigation on the impact of compromised master nodes is left as future work.

System assumptions: We present our assumptions about the sensor network environment as follows:

- **Periodic data collection:** Time divided into equal and fixed collection rounds and each sensor nodes collects a single data unit per round
- **Unattended operation:** An itinerant sink periodically visits the UWSN to collect sensed data. There is a system wide parameter-v-denoting the maximum number of collection rounds between successive sink visits
- **Communication:** The UWSN is always connected and any two sensors can communicate either directly or through peers, according to the underlying routing protocol
- **Storage:** each sensor nodes has enough storage for O (v) data units
- **Cryptographic capabilities:** Each sensor can perform 160-bits Elliptic Curve Cryptography
- **Adversary power:** μADV can erase no more than k of measurements from the network. Erasing more than that, raises an alarm on the sink and contradictsμADV's goal of remaining undetected
- **Re-initialization:** At each visit, the sink re-initializes the network, empty master nodes storage and reset the round counter

THE PROPOSED CADS SCHEME

Our goal is to provide various mechanisms for ensuring and maintaining the security and dependability of sensed data under the aforementioned adversary model. Specifically, we have the following goals: (1) Security: To enhance data confidentiality and integrity by increasing the attacker's cost, decreasing the gain on compromising individual sensors. (2) Dependability: To enhance data availability against both sensor Byzantine failures and sensor compromises and minimize the effect brought by individual sensor failures and compromises. (3) Dynamic Integrity Assurance: We should be able to ensure the distributed data shares are correctly stored over the interval, thus can finally be used to reconstruct the original data by authorized users. (4) Lightweight: The scheme design should be lightweight as always in order to fit into the inherent resource-constrained nature of WSNs.

Achieve all these goals. On the one hand, efficient distributed data storage system should exploit to solve single node of failure. On the other hand, effective cryptographic primitives are needed to ensure data integrity and communication privacy due to sabotage of adversary.

Preliminaries: We now introduce some necessary background for our proposed scheme:

Secret sharing: Shamir proposed an (n, k) secret sharing threshold scheme (Shamir, 1979) based on polynomial interpolation, in which k of n shares of a secret are required to reconstruct the secret. This Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate. By properly choosing the n and k parameters, it can give any sufficiently large majority the authority to take some action while giving any sufficiently large minority the power to block it.

Discrete Logarithm Problem (DLP): DLP typically involves recovery of $x \in Z_p$, given p, g and g^x (mod p), where, p is a prime integer and g is a generator of Z_p. Given any x, compute $y \equiv g^x$ is easy. However, given any y, find a g such that $y \equiv g^x$ (mod p) is difficult (Yan, 2003).

We follow the conventional assumption that master, sensor nodes know their geographic locations through many existing techniques and the clocks of sensor nodes in a network are loosely synchronized based on an attack-resilient time synchronization protocol (Song *et al*., 2007). The two-tier architecture is indispensable for increasing network capacity and scalability, reducing system complexity and prolonging network lifetime (Desnoyers *et al*., 2005).

To guarantee the security of the stored data, sensor nodes must encrypt the data for confidentially. Thus, only authorized user can obtain the access privilege and decrypt the data information. In addition, as sensors may exhibit Byzantine behaviours and are attractive for attacks, data dependability should also be ensured to avoid single point of failure. The process of our CADS scheme comprises two phases: secret distribution and secret reconstruction with the dynamic integrity verification. For clarity, we list the symbols used in this study below:

- v, w, P_i ($i \in \{1,\ldots,n\}$): v and w are regular sensor nodes. P_i is the set of neighbours of v within its transmission range
- S, S_i ($i \in \{1,\ldots,n\}$): S denotes original data on each sensor and S_i denotes data shares for each P_i generated by secret sharing scheme
- y, y_i ($i \in \{1,\ldots,n\}$): check value before and after employing g, S or S_i, respectively
- k^i_r, k^i_p, k^i_s: k^i_r is the session key shared between i-th sensor and sink in round r, k^i_p, k^i_s is public key pair of i-th sensor
- E (k, m): encrypt information m with key k
- a_i: primitive element randomly select from Z_p
- U_r: set of data items undecipherable by adversary in round r

Secret distribution: Suppose a sensor node v has data to be stored locally, we assume that the data original sensor is honest and not compromise by adversary yet. All participators submit their data at the same time to prevent colluding attacks. To protect data, it perform the following operations to ensure the data integrity and confidentially.

Step 1: Generate a random session key k^v_r, compute the keyed hash value h (data, k^v_r) of data

Step 2: Encrypt h (data, k^v_r), data with k_r and obtain {data, h (data, k^v_r)} k^v_r

Step 3: Store S=< {data, h (data, k^v_r)} k^v_r}> and destroy k^v_r

Step 4: v then picks a random k-1 degree polynomial $f(x) = a_0+a_1x+\ldots a_{k-1}x^{k-1}$, in which a_0=S and employs a (n, k) secret sharing to obtain n shares of S, denoted as S_i = f (i) mod p ($1 \le i \le n$), v further compute $y = g^s \bmod p$, $y_i = g^{S_i} \bmod p$

Step 5: v disclose y, y_i to the network and distributes S_i to p_i ($1 \le i \le n$), the original data S is erased

By accomplishing the above process, secret shares are generated and distributed to its share holders.

Secret reconstruction: The inverse process is implemented at the end of each round, to make this process more secure, we assume public key cryptography is used and master nodes know each sensor's private key.

Step 1: For each p_i ($1 \le i \le n$), generates $Ci = E(k^i_p, y \| S_i)$, sends C_i to master nodes

Step 2: After received corresponding message, master node first decrypt C_i with k^i_s, verify $h_i \stackrel{?}{=} g^{S_i} \bmod p$, if the equation not holds, then p_i is cheating, else

Step 3: Master node employing Lagrange interpolation polynomial to derive the secret data S:

$$f(0) = S = \sum_{i=1}^{k} S_i \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{j}{j-i} \bmod p$$

Since, the data are finally collected by master nodes, the verification process is performed by master nodes, however, our scheme also enable each share holder to verify the integrity of data shares.

Data maintenance: In our storage scheme, the original data block is first partitioned into n shares of equal size using secret sharing. Based on these shares, additional n verification messages are generated. By distributed each neighbour a distinct data share with a public check message, as long as at most k blocks are in error, then the original data shares can be determined whenever $k \le n/2$. Once any unauthorized data modification is detected, to repair the polluted shares, the mobile sink can be applied to collect data shares and perform error correction. Due to the space limitation, in this study we only focus on the secure data storage scheme with dynamic data integrity check. The issue of data maintenance will be addressed in detail in our future work.

ANALYSIS AND PERFORMANCE RESULTS

Security analysis: Let us now assume that k-1 of these n pieces are revealed to an opponent. For each candidate value S' in [0, p), he can construct one and only one polynomial f'(x) of k-1 such that f' (0) =S' and f' (i) =S_i for the k-1 given arguments. By construction, these p possible polynomials are equally like. Compromising less than k sensors will not damage data security and dependability. Thus, it is absolutely nothing that the opponent can deduce about the real value of S. Our scheme takes advantage of several benefits: First, data share is confidential and secure protect, we utilize discrete logarithm problem, therefore, public y, y_i does not expose the secret S, S_i to the adversary. In fact, from y and y_i to deduce S, S_i is equivalent to solve the hardness of discrete logarithm problem. Second, secret holders cannot success of cheat, given $\forall I \neq j$ ($1 \leq i, j \leq p-1$), it always has $g^i \neq g^j$, receiver can verify $y_i = g^{S_i} \bmod p$ to detect cheating. Last but not least, public key cryptography is used to ensure data security during the transmission process, each sensor use the master node's public key encrypted the message, while private key is only hold by master node which have tamper-proof hardware, thus compromise master node is impossible in our work

Performance results: We assume that sensors deployment follow a two-dimensional Gaussian distribution, our methodology should be easily adaptable to other deployment models. The number of normal sensor nodes and master nodes in a grid cell is 30, 1 respectively. The deployment area is 800×800, with each cell of size 80×80 m. The wireless communication range for a sensor node and a master node is 40, 120 m, respectively. Each sensor nodes collects a single data unit per round. We evaluate the data availability and false negative probability compared to propose scheme in (Pietro *et al*., 2009b). It used MOVE-ONCE and KEEP-MOVING strategies to hide the secret, that is:

MOVE-ONCE: At every round r, each sensor randomly picks a neighbour sensor and sends data to it until the next sink visit.

KEEP-MOVING: At each round r each sensor moves each hosted data item separately, i.e., for each data item that stores (and collects), it picks random sensors and moves there the stored item.

We assume the adversary can compromise at most m = 10 sensors per round. For every scenario, we run the simulation 100 times: a simulation lasts for 50 rounds. We define the data survival quantity as the average numbers

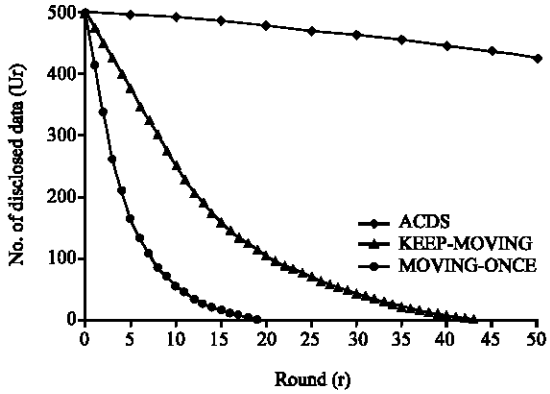

Fig. 2: Number of data survival in ACDS, KEEP-MOVING and MOVING-ONCE

of ciphertexts or data shares that μADV was unable to distinguish from a target data in each round, that is, the data is still undisclosed to adversary. Figure 2 plots the number of data undisclosed to adversary. It clearly shows that, the data survival quantity of ACDS is significant higher than other two schemes, with public key encryption and MOVE-ONCE or KEEP-MOVING, a powerful adversary sooner or later would break it and derive the secret, these two survival strategies vary only as far as exactly how many rounds it takes adversary to win. With MOVING-ONCE strategy, the data survival is drastically decreased, it only takes 19 rounds for the adversary to compromise all the data in the network and relatively more rounds of 43 to compromise all the data with KEEP-MOVING strategy. However, with secret sharing technique in our scheme, the number of data successfully received by master nodes is significant larger than these two schemes, with a smooth decrease due to some of sensor nodes are compromised, but the master node still can receive enough data shares to reconstruct the original data. The adversary failed to derive more information other than compromised sensor nodes. The performance results well support our design principles and in accordance to our goals. Because we take advantages of secret sharing technique to divide data into n pieces so that providing redundancy for original data components. Here the n shares are not the simple fragmentation of a message, but a mathematical transformation such that each individual share does bear information about the message, while not carry any meaningful partial plain text of the original message. Even with powerful adversary with infinite computing time, if the number of shares available is less than k, the cheater can do no better than guessing (Caballero and Hernandez, 2006). Compromising less than k sensors will not damage data security and dependability and the adversary cannot

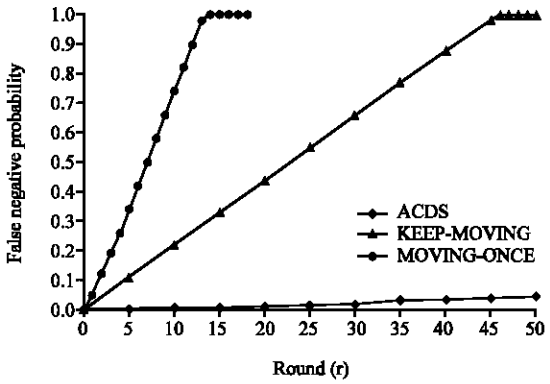

Fig. 3: False negative probability of ACDS, KEEP-MOVING and MOVING-ONCE

success of cheat after compromised a sensor node. The greater the size of U_r, the higher the probability that the target data will persist until the next sink visit.

We consider the adversary simply modified the data and sent to the next hop. The false negative probability is defined as the probability that the master node cannot distinguish forged data from sensor nodes. We compare the false negative probability of ACDS scheme with MOVING-ONCE and KEEP-MOVING schemes with the same network settings. Note that data reconstruction operation is only performed on the master node in ACDS. As showed in Fig. 3, the false negative probability of MOVING-ONCE is highest among three schemes, about 13 rounds after network running, the master node failed to distinguish correct data in the network due to sensor compromise and no redundancy data provided. KEEP-MOVING strategy takes relative longer of 45 rounds appear completely lose to receive correct data. Finally, our ACDS can achieve almost zero false negative compared to the above two approaches. As discussed earlier, since MOVING-ONCE and KEEP-MOVING strategies by Pietro *et al.* (2009b) just move the data randomly, result in forwarding the data to nodes that have been captured. Hence, increase the probability of false negative. With dynamic integrity verification based on discrete logarithm problem in our work, there is an overall identifying code y and local identifying code y_i corresponding to each data share known to public, all sensor nodes can easily verified the data shares fabricated by adversary. Therefore, our proposal can achieve the lowest false negative probability. The results again confirm the previous discussion and our original intention.

RELATED WORKS

A more recent result addressing data availability in WSNs by Mathur *et al.* (2006). It develops a scheme to maximize the amount of data recovered by the sink and shows how the proposed scheme improves data availability when a portion of the network is invalidated by natural disasters, such as a flood or an earthquake. In (Girao *et al.*, 2007), the authors regarding secure distributed data storage can be found in the literature, but none of them satisfies the overall requirements of data confidentiality, dependability, integrity and efficiency. Song *et al.* (2005) proposed a secure data access approach by using polynomial-based key management scheme, where the sinks can retrieve the network data following the fixed routes. Subramanian *et al.* (2007) studied the distributed data storage and retrieval problem in sensor networks and designed an adaptive polynomial-based data storage scheme for efficient data management. However, both of these schemes do not consider the data dependability and integrity. Chessa and Maestrini (2003) investigated the data storage problem in the context of Redundant Residue Number System (RRNS). Subbiah and Blough (2005) developed a novel combination of XOR secret sharing and replication mechanisms, where each share is managed using replication-based protocols for Byzantine and crash fault tolerance. A work that deals with the concept of unattended networks is pDCS (Shao *et al.*, 2008). There, the authors propose a scheme for Data-Centric Sensor Networks that leverages the notion that the nature of the data is more important than the identities of the nodes that collect the data. Those networks can be considered Unattended since their data spread across the entire network and it is queried on demand, while sensors want to protect their data against several types of attacks.

CONCLUSION

In this study, we propose a co-operative and anti-fraud data storage scheme with dynamic assurance in unattended wireless sensor networks. We utilize secret sharing in the initial data storage process to guarantee data confidentiality and dependability. To ensure the integrity of data shares, an efficient dynamic data integrity checking scheme is constructed based on the principle of discrete logarithm problem. In contrast to existing approaches, higher data survival quantity and perfect zero false negative probability are achieved in our scheme. Furthermore, through security analysis and performance, we show that our scheme is highly secure and efficient, thus can be implemented in the current generation of sensor networks.

ACKNOWLEDGMENTS

This study was partially or fully supported by National Basic Research Program of China (973 Program)

under Grant No. 2006CB303000 (2006.9-2011.8, Hunan University) ,2009CB326202 (2009.4-2011.8, Hunan University) and 2010CB334706 (2010.4-2013.3, Hunan University). Key Program of National Natural Science Foundation of China under Grant No. 60736016 (2008.1-2011.12, Hunan University). National Natural Science Foundation of China under Grant No.60873198 (2009.1-2011.12, Hunan University), 60973128 (2010.1-2012.12, Hunan University) and 60973113 (2010.1-2012.12, Hunan University). Scientific Research Fund of Hunan Provincial Education Department under Grant No. 09C403 (2009.6-2012.6, Hunan University of Science and Technology), National Natural Science Foundation of Hunan Province and Xiangtan united Foundation under Grant No. 09JJ9006 (2009.6-2012.6, Hunan University of Science and Technology), Key Program of Scientific Research Fund of Hunan Provincial Education Department under Grant No. 09A027 (2009.6-2012.6, Hunan University of Science and Technology).

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Bairaktaris, K., L. Chatziqiarmakis, V. Liagkou and P.G. Spirakis, 2008. Adaptive probabilistic secure routing in mobile wireless sensor networks. Proceedings the 16th International Conference on Software, Telecommunications and Computer Networks, Sept. 25-27, Computer Technology Institute, Patras, pp: 208-212.

Benenson, Z., F.C. Freiling and P.M. Cholewinski, 2007. Advanced evasive data storage in sensor networks. Proceedings International Conference on Mobile Data Management, May 1, IEEE Computer Society, Washington DC, USA., pp: 146-151.

Caballero, P. and C. Hernandez, 2006. Secret sharing based on hard-on-average problem. Linear Algebra Appl., 414: 626-631.

Chan, H., P. Adrian and S. Dawn, 2003. Random key predistribution schemes for sensor networks. IEEE Symposium on Research in Security and Privacy, May 11-14, IEEE Computer Society, Washington, DC., pp: 197-213.

Chessa, S. and P. Maestrini, 2003. Dependable and secure data storage and retrieval in mobile, wireless networks. Proceedings of Dependable Systems and Networks, June 22-25, Universita Pisa, pp: 207-216.

Desnoyers, P., D. Ganesan and P. Shenoy, 2005. SAR: A two tier sensor storage architecture using interval skip graphs. Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, Nov. 2-4, San Diego, California, USA., pp: 39-50.

Du, X., Y. Xiao and H. Chen, 2009. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. IEEE Trans. Wireless Commun., 8: 1223-1230.

Girao, J., D. Westhoff, E. Mykletun and T. Araki, 2007. Tinypeds: Tiny persistent encrypted data storage in asynchronous wireless sensor networks. Ad Hoc Networks, 5: 1073-1089.

Hara, T. and S.K. Madria, 2006. Data replication for improving data accessibility in ad hoc networks. IEEE Trans. Mobile Comput., 5: 1515-1532.

Kahn, J.M., R.H. Katz and K.S.J. Pister, 1999. Next century challenges: Mobile networking for smart dust. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Aug. 15-19, Seattle, WA., pp: 271-278.

Kamra, A., V. Misra, J. Feldman and D. Rubenstein, 2006. Growth codes: Maximizing sensor network data persistence. Comput. Commun. Rev., 36: 255-266.

Kariof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Proceedings of the 1st International Workshop on Sensor Network Protocols and Applications, May 11, California University, Berkeley, CA, USA., pp: 113-127.

Konoma, C., M. Mambo and H. Shizuya, 2005. The computational difficulty of solving cryptography primitive problems related to the discrete logarithm problem. IEICE Trans. Fundam. Electronics Commun. Comput. Sci., 88: 81-88.

Mache, J., C.Y. Wan and M. Yarvis, 2008. Exploiting heterogeneity for sensor network security. Proceedings of Sensor, Mesh and Ad Hoc Communications and Networks, June 16, San Francisco, USA., pp: 591-593.

Madria, S. and J. Yin, 2009. SeRWA: A secure routing protocol against wormhole attacks in sensor networks. Ad Hoc Networks, 7: 1051-1063.

Mathur, G., D. Peter, G. Deepak and S. Prashant, 2006. Capsule: An energy-optimized object storage system for memory-constrained sensor devices. Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, Oct. 31-Nov. 3, Boulder, Colorado, USA., pp: 195-208.

Meng, L., W. Fu, Z. Xu, J. Zhang and J. Hua, 2008. A novel Ad hoc routing protocol based on mobility prediction. Inform. Technol. J., 7: 537-540.

Pietro, R.D., D. Ma, C. Soriente and G. Tsudik, 2008a. POSH: Proactive cooperative self-healing in unattended wireless sensor networks. Proceedings of IEEE Symposium on Reliable Distributed Systems, Oct. 6-8, Naples, pp: 185-194.

Pietro, R.D., L.V. Mancini, C. Soriente, A. Spognardi and G. Tsudik, 2008b. Catch me (if you can): Data survival in unattended sensor networks. Proceedings of 6th Annual IEEE International Conference on Pervasive Computing and Communications, March 17-21, Hong Kong, Rome, pp: 185-194.

Pietro, R.D., C. Soriente, A. Spognardi and G. Tsudik, 2009a. Collaborative authentication in unattended sensor networks. Proceedings of the 2nd ACM Conference on Wireless Network Security, March 16-19, Zurich, Switzerland, pp: 237-244.

Pietro, R.D., L.V. Mancini, C. Soriente, A. Spognardi and G. Tsudik, 2009b. Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks. Ad Hoc Networks, 7: 1463-1475.

Raymond, D.R. and S.F. Midkiff, 2008. Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Comput., 7: 74-81.

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613.

Shao, M., W. Zhang, G. Cao and Y. Yang, 2008. PDCS: Security and privacy support for data-centric sensor networks. IEEE Trans. Mobile Comput., 8: 1023-1038.

Song, H., S. Zhu, W. Zhang and G. Cao, 2005. Least privilege and privilege deprivation: Towards tolerating mobile sink compromises in wireless sensor networks. ACM Trans. Sensor Networks, 4: 591-625.

Song, H., S. Zhu and G. Cao, 2007. Attack-resilient time synchronization for wireless sensor networks. Ad Hoc Networks, 5: 112-125.

Subbiah, A. and D.M. Blough, 2005. An approach for fault tolerant and secure data storage in collaborative work environments. Proceedings of ACM Wrokshop on Storage Security and Survivability, Nov. 11, Fairfax, VA, USA., pp: 84-93.

Subramanian, N., C. Yang and W. Zhang, 2007. Securing distributed data storage and retrieval in sensor networks. Pervasive Mobile Comput., 3: 659-676.

Wei, D., H.A. Chan and B. Silombela, 2007. Rectangular grids design to balance power consumption for homogeneous sensor networks with high node density. Inform. Technol. J., 6: 827-834.

Yan, S.Y., 2003. Computing prime factorization and discrete logarithms: From index calculus to xedni calculus. Int. J. Comput. Mathematics, 80: 573-590.

Yu, Z. and Y. Guan, 2008. A key management scheme using deployment knowledge for wireless sensor networks. IEEE Trans. Parallel Distributed Syst., 19: 1411-1425.