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 10 (7): 1359-1366, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1359.1366

An Efficient Data Delivery Mechanism by Exploring Multipath Routes for Wireless Sensor Networks

[1]Zhiqiang Ruan and [1,2]Xingming Sun
[1]Hunan Provincial Key Laboratory of Network and Information Security,
Hunan University, Hunan Changsha, 410082, China
[2]Jiangsu Engineering Center of Network Monitoring,
Nanjing University of Information Science and Technology, China

Abstract: This paper study the data delivery mechanisms that can with high probability thwarting node capture attacks in unattended or distributed wireless sensor networks. Classic cryptographic approaches are vulnerable to such attacks, mainly due to their deterministic nature. Because once the adversary compromises the sensor nodes, it can acquire the credential as well as the data collected and held by sensors. Furthermore, the adversary can easily insert bogus sensor readings or change the processing results and then use these keys to authenticate forged information. This study proposes and analyzes the application of Reed-Solomon (RS) codes to address the problem. In the proposed scheme, each sensor node encodes the original data into multiple redundancy data shares by applying predefined (n, k) RS codes and applies non-uniform allocation through multiple node-disjoint paths to the destination. Analysis and simulation results demonstrate that the proposed scheme is efficient and resilient against node capture attack.

Key words: Wireless sensor network, data delivery, node capture, fault tolerant, probabilistic analysis

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, hazard leak detection and battlefield sensing. Security issue is still in its early stage of development. Of the various possible security threats encountered in a wireless sensor networks, this study specifically interested in combating compromised-node attacks (Meng *et al*., 2008). Due to the unattended nature of WSNs, an adversary can physically compromise a subset of nodes to eavesdrop information; they can interfere with the normal operation of the network by actively disrupting, changing, or even paralyzing the functionality of a subset of nodes. One important feature that separates it from other adversarial models is its mobility (Ruan *et al*., 2010). Specifically, the adversary has one central goal: to prevent certain data collected by sensors from ever reaching the sink or provide forged information to mislead the user to make incorrect decisions.

Existing approaches are achieved by cryptographic techniques (Wei *et al*., 2007) or watermarking method (Wang *et al*., 2011). However, due to the limited resource of sensor nodes coupled with the unattended operation of such networks, an adversary who can potentially capture nodes, recover their cryptographic material. Internal adversaries (or compromised nodes) can further alter and insert bogus data and pose as an authorized node in the network. If the sensor networks deployed in hostile environment and always provides highly valuable information to the end user but when most of the information has been forged and misleads the user to make incorrect decisions (Ruan *et al*., 2010). Attaching message authentication codes can verify the modification of data but cannot verify its validity (Wang *et al*., 2011). In general, the conventional view of security based on cryptography and authentication alone is not sufficient to provide a complete solution for developing secure and dependable sensor data delivery mechanism due to the unique characteristics and novel misbehaviours encountered in unattended sensor networks.

The intent of this work is to develop an efficient in-network data delivery mechanism for sensor data, while simultaneously robust to stop forwarding as well as filtering out bogus data. The work is motivated from the well studied secret sharing and multipath routing. The strategy is for each node to partition the original data into multiple redundancy data shares by applying predefined

Corresponding Author: Zhiqiang Ruan, Hunan Provincial Key Laboratory of Network and Information Security,
Hunan University, Hunan Changsha, 410082, China Tel: 86-025-58731575

Reed-Solomon (RS) codes (Goodson *et al.*, 2004) and utilize non-uniform allocation of data shares through multiple node-disjoint paths to the sink. It is noted that the proposed scheme does not eliminate the utilization of any conventional cryptography approaches, such as data encryption and pairwise key establishment and it works as a complementary component to provide an enhanced security solution with the imperfect unattended WSN.

PRELIMINARIES

This section gives the preliminaries to be used in this study. For the sake of clarity and convenience description, the notations used in the following sections are given in Table 1.

The (n, k) codes are used to share secrets among n users, any k of which can recover the secret cooperatively. The Shamir scheme (Shamir, 1979) is one of such schemes. As pointed out in (Goodson *et al.*, 2004), an RS code may be treated as a special (n, k) secret-sharing scheme with tamper-resistant capability, because it can correct errors.

Let GF(2^a) be the finite field of order 2^a such that each element in GF(2^a) can be represented by *a* bits. An (n, k) RS code is a linear code, where each symbol is in GF(2^a), with parameters: $n = 2^a-1$ and $n-k = 2t$, where n is the total number of code symbols in the coded block, k is the total number of information symbols and t is the symbol-error-correcting capability of the code. Let m(x) be the information polynomial represented as $m(x) = m_0+m_1x+\ldots+m_{k-1}x^{k-1}$, where m_i is a *a* bits code.

The codeword polynomial c(x) corresponding to m(x) can be encoded as:

$$c\ (x) = b\ (x)+x^{2t}\ m\ (x) \tag{1}$$

Where:

$$b\ (x) = x^{2t}\ m\ (x) \bmod g\ (x) = b_0+b_1x+\ldots+b_{2t-1}x^{2t-1} \tag{2}$$

is the parity check polynomial and g(x) is a publicly known generator polynomial which can be obtained as:

$$g\ (x) = (x+\beta)\ (x+\beta^2)\ldots(x+\beta^{2t}) = g_0+g_1x+g_2x^2+\ldots g_{2t}x^{2t} \tag{3}$$

where, β is a primitive element in GF(2^a) and $g_i \in GF(2^a)$, note that g(x) has β, β^2, …, β^{2t} as roots.

Since each symbol is represented by a bits, an (n, k) RS code can be expended to a (an, ak) binary linear block code. For example, a (17, 9) RS code with four symbol-error-correcting capabilities is of 8×9 = 72 information bits. The computational cost of encoder is roughly k(n-k) additions and k(n-k) multiplications.

Table 1: Notations summary

Variables	Definitions
n	The number of total symbols of RS code
k	Total number of information symbols of RS code
a	nonzero elements in the finite field
t	Symbol-error-correcting of RS code
m	The number of available paths
c	The code word of an (n, k) RS code
f_j	Fraction of symbols transmitted on jth path
h_j	The hop count of the jth path
x	The probability of sensor compromised
r_T	The number of total routers in all paths
r	The number of sensor compromised
m_x	The number of path compromised
p_x	The probability of data compromised

The decoding processes of RS code are more complex. Let $r(x)=r_0+r_1x+\ldots+r_{k-1}x^{k-1}$, $e(x)=e_0+e_1x+\ldots+e_{k-1}x^{k-1}$, $c\ (x)=c_0+c_1x+\ldots+c_{k-1}x^{k-1}$, where e_i, r_i, $r_i \in GF\ (2^a)$, r (x) is the received polynomial, e (x) is error polynomial and c (x) is original data polynomial, then e (x) = r (x)-c(x). From Eq. 1-3 it is known that the roots of g(x) must also be the roots of c (x), r (x) evaluated at each of the roots of g (x) should yield zero only when it is a valid codeword. Any errors will result in one or more of the computations yielding a nonzero result. The computation of a syndrome symbol can be described as follows:

$$S_i = r\ (\beta^i) = \sum_{j=0}^{n-1} e_j\beta^{ij} \text{ for } i=1,\ldots,2t. \tag{4}$$

If there exists v errors, where $0 \le v \le t$, in the unknown locations j_1, j_2, …, j_v of the received polynomial. Then:

$$e\ (x) = e_{j1}x^{j1}+e_{j2}x^{j2}+\ldots+e_{jv}\ x^{jv} \tag{5}$$

Define the error values to be $Y_l=e_{j1}$, where l = 1, 2, ... , v and the error locators to be $X_l=\beta^{jt}$, where l = 1, 2, …, v. Utilize Forney's algorithm (Lin and Costello, 2004) to derive the error values Y_l. Thus, the error correcting polynomial:

$$e(x) = \sum_{l=1}^{v} Y_l x^{jl} \tag{6}$$

To recover the original data c (x), using

$$c\ (x) = r\ (x)-e\ (x) \tag{7}$$

THE PROPOSED SCHEME

Description of the Proposed scheme: This study uses symbols or shares interchange and the concept of node or path compromising characteristics gives as follows:

- **Definition 1:** Given a path (s, e) consisting of nodes s, n_1, n_2, …, n_l, e, define (s, e) is compromised as when any one or more of the nodes from n_1 to n_l is compromised. Otherwise, if (s, e) were not compromised, all data shares on (s, e) would be safe.
- **Definition 2:** Given two node-disjoint paths p_i and p_j, $i \neq j$, compromise p_i is independent of p_j.

According to Definition 1, the cost of sending a packet through one path is proportional to its hop count, more importantly, as the length of a multi-hop path increases, the possibility of path compromise is higher. Definition 2 shows the benefit of using node-disjoint path. Note that a compromised source makes the data delivery scheme meaningless, thus it is reasonable to assume that the source are trustworthy.

Let c= (c_0 , c_1,…, c_{n-1}) be a codeword of an (n, k) RS code over GF(2^a), where $c_i \in$ GF (2^a) ($1 \leq i \leq n$) is a symbol. Here, c_0, c_1, …, c_{n-1} are the information that the sensor node needs to send to the destination node or sink. Since an (n, k) RS code can recover up to t=(n-k)/2 errors, n should satisfy n=k+2t.

In order to minimize transmission overhead and simultaneously maximize the security of the scheme, the sender should choose an appropriate value of (n, k) and send different numbers of symbols through difference paths according to their hop counts and path quality. The select of (n, k) reflect the security requirement of the user and the symbol allocation on path reflects the current condition of the network. Assume that basic security mechanisms such as pairwise key establishment between two neighbouring nodes (Ren *et al*., 2011) are already in place to provide basic communication security.

Suppose a sensor node U has data D to be sent to destination M. Without loss of generality, to secure D, basic encryption and integrity operation are performed before applying RS coding scheme.

The operational procedures of the proposed scheme given as follows:

- U generates ciphertext as S =< {D‖ h (D, k_r), where h (D, k_r) is the keyed hash value and k_r is the key shared between M and U. Note that the key k_r can be either symmetric or asymmetric depending on the chosen access control mechanism, which is independent to the design here and will not be discussed in this study.
- U then constructs m (x) = $m_0+m_1+\ldots+m_{k-1}x^{k-1}$, where S : = { m_0‖m_1, …, m_{k-1}}. U further encodes k symbols {m_0, m_1, …, m_{k-1}} into a codeword with n symbols c= (c_0, c_1,…, c_{n-1}) using Eq. 1-3.
- U generates m node-disjoint paths between U and M; the procedure of establishing such secure paths is out of the scope of this study (Lou and Fang, 2001; Papadimitratos and Haas, 2006; Lou and Kwon, 2006).
- U uses source routing to send at most q_jn symbols on each path j for $1 \leq j \leq m$. If q_jn is not an integer, a round off value will be used instead. The original data is then securely erased.
- Assume M receives all symbols from the m paths, M uses majority rule to eliminate bad symbols and composes received data polynomial r (x).
- M identifies faulty path by evaluating Eq. 4 and 5 and uses Forney's algorithm (Lin and Costello Jr., 2004) to derive error polynomial e(x) using Eq. 6.
- M recovers D by reconstructs {D ‖ h (D, k_r)} k_r from c (x) using Eq. 7 any k out of n symbols is sufficient for derive the original polynomial.
- M decrypts {D ‖ h (D, k_r)} k_r with shared key k_r and verified the data D, if it is verified, the transmission of the data has succeeded. Otherwise, if the decode process fails due to more than t errors, an alarm report is supposed to release to the network owner

Note that the proposed scheme does not need know the identification of the compromised paths to decode the data successfully. The RS decoder at the destination node will automatically correct any modification by the compromised nodes in these paths.

Non-uniform allocation: Assume that the sender transmits f_j fraction of the total n symbols through path j, where $1 \leq j \leq m$ and

$$\sum_{i=1}^{m} f_{j} = 1$$

Due to the lack of the knowledge of which paths may be compromised, the sensor node has the best option of making sure that the expected number of symbols compromised on each path is more or less the same.

Let h_j be the hop count of path j, $1 \leq j \leq m$ and x the probability of nodes being compromised, given that the source and destination are not compromised, the probability that path j is compromised is:

p_j = Pr (at least of one node in between the path is compromised):

$$= 1\text{- Pr (none of the nodes is compromised)} = 1-(1-x)^{h}{}_{j-1}$$

where $1 \le j \le m$. The expected number of symbols being compromised for path j is $f_j p_j$ and the source node needs to make sure that $f_j p_j = C$, for all j. That is,

$$f_j . [(1-(1-x)^{hj-1}] = C \qquad (8)$$

Since $\sum_{j=1}^{m} f_j = 1$, the constant C should satisfy

$$C = \frac{1}{\sum_{i=1}^{m} \frac{1}{1-(1-x)^{h_j-1}}}$$

As mentioned earlier, the probability of path compromise is in proportion to the length of multi-hop path. It only need to derive the relation between f_j and h. when x is small, then

$$1-(1-x)^{h_j-1} \approx 1-[1-(h_j-1)x] = (h_j-1)x$$

Therefore, C becomes

$$C \approx \frac{x}{\sum_{i=1}^{m} \frac{1}{h_i - 1}} \qquad (9)$$

According to Eq. 8 and 9, then

$$f_j \approx \frac{C}{(h_j-1)} = \frac{\frac{1}{h_j-1}}{\sum_{i=1}^{m} \frac{1}{h_j-1}} \qquad (10)$$

Thus, a closed form for f_j, $1 \le j \le m$, which is related to h, is derived.

ANALYSIS AND SIMULATION

Analysis: Under the supposed adversary model, the data compromise probability p_x, which is define as the probability of compromising enough symbols to the adversary so that it can obtain the data with relative ease when the node compromised probability is x ($0 \le x \le 1$).

Let $m = s_2+s_3+...+s_L$, where s_2, s_3 , …, s_L, represented the source node find s_2 paths of length (hops count) 2, s_3 paths of length 3, … and s_L paths of the maximum length L (note that all these paths are node-disjoint paths). Let $m_x = n_2+n_3+...+n_L$, where m_x is the number of paths among m available paths that are compromised by the adversary, which contains n_2, n_3, ... n_L number of paths among s_2, s_3,... s_L that are compromised, respectively. More specifically, assume that n_{j1}, n_{j2},..., n_{jg}, $0 \le g \le L-1$, are the nonzero term of n_2, n_3, ... n_L. Therefore, they are n_{j1} paths of length j_1 compromised; n_{j2} paths of length j_2 compromised…, n_{jg}paths of length j_g compromised.

When the multiple node-disjoint paths are used, the source node transmits n symbols through the m paths with f_j fraction for path j, $1 \le j \le m$, where f_j is given by Eq. 10. Define the data compromise probability of the proposed scheme as the probability of at least k symbols being compromised to the adversary. For comparison between the proposed scheme and single path scheme, this study uses p_x^{our} to distinguish from single path scheme, which uses p_x^{sp} . Therefore, the data compromise probability can be calculated as:

P_x^{our} = [The overall probability of compromising r nodes]
×[The overall probability of compromising ni paths]
× [The probability of at least one node on each compromised path is compromised] = p1×p2×p3

Since all found paths are node-disjoint, the total number of nodes between source node and storage node is:

$$r_T \sum_{i=2}^{L} (i-1) S_i \qquad (11)$$

Based on the independent compromised probability x, the probability that r out of r_T nodes are compromised is

$$\binom{r_T}{r} x^r (1-x)^{r_T - r} \qquad (12)$$

Hence, the overall probability of compromising r nodes is

$$p_1 = \sum_{r=1}^{r_T} \binom{r_T}{r} x^r (1-x)^{r_T - r} \qquad (13)$$

Now, the overall probability of compromising n_i paths (p_2) can be calculated as follows: there are n_i paths among s_i of length i are compromised, according to definition 2, each path is independent of another, with total of m_x compromised paths, p_2 can directly derive as:

$$p_2 = \sum_{n_2+n_{3+...+n_L=m_x}} \prod_{i=2}^{L} \binom{S_i}{n_i} \qquad (14)$$

where $0 \le n_i \le s_i$ for $2 \le i \le L$.

According to definition 1, a path is compromised due to one or more than one node on the path is compromised, that is, r = $m_{x.}$ Considering all possibilities to select r compromised nodes from $x_n = \sum_{i=1}^{g} n_{ji}(j_i - 1)$ nodes on the m_x compromised paths. Hence, the probability of at least one node on each compromised path must be compromised is:

$$p_3 = \sum_{y1,1+...+y1,n_{ji}+y_{2,1}+...+y_{2,nj2}+...+y_{g,1}+...+y_{g,njg}=r} \frac{\prod_{i=1}^{g} \prod_{l=1}^{n_{ji}} \begin{pmatrix} j_{i-1} \\ y_{i,1} \end{pmatrix}}{\begin{pmatrix} r_T \\ r \end{pmatrix}} \quad (15)$$

where $1 \leq y_{i,1} \leq j_i$-1 for $1 \leq i \leq g$.

Therefore, the data compromised probability p_x^{our} can be calculated by Eq. 12-15.

For fair comparison, the data compromise probability in single path (SP) scheme p_x^{sp} also calculated. In the SP scheme, the data are transmitted through one randomly chosen path among the m available paths. If it selects a compromised path to transmit, then the whole data is revealed. Hence, when there are m_x compromised paths, the data compromised probability is m_x / m. Then:

$$p_x^{sp} = \sum_{r=1}^{r_T} [\begin{pmatrix} r_T \\ r \end{pmatrix} x^r .(1-x)^{r_T - r} \sum_{m_x=1}^{m} P_3 . \frac{m_x}{m}] \quad (16)$$

where, r_T is given by Eq. 11 and p_3 is given by Eq. 15.

Simulation results: Simulations have been performed in NS-2 to evaluate the efficiency of the proposed scheme under the threat model. Unless specified otherwise, simulations were set up with the following parameters: N = 800 nodes are randomly placed on a square area of 500 m by 500 m. The area is divided into a gird of 25 = 5×5, with each grid cell of size 100m×100m. The radio transceiver range of each sensor node is 40m. The RS code is assumed to be (n, k) = (17, 9).

In order to understand the benefit of using node-disjoint paths serving in defending against of node capture, Fig. 1 investigated the probability of data compromised p_x as a function of node compromised probability x. It artificially decreased N, with half the nodes (N = 400) and allow the source node to randomly select all available paths during the path selection process for comparison purposes. Assume each sensor node has equally likely to be compromised with probability *x*, x = 0.01, ..., 0.09. Based on Fig.1, it can be concluded that under the same node density N (N = 400 or N = 800), the probability of data compromised increases with node compromised probability and given the same node compromised probability x, the proposed scheme using enhanced node-disjoint paths outperform randomly selected paths scheme with lower data compromised probability. An example of these results is that when N = 800 and x = 0.07, the corresponding p_x is 0.39 and 0.1, respectively. It can further conclude that with a larger N, there have a relatively more neighbours, increasing potential more node-disjoint paths. Note that the proposed scheme uses shortest and trust-aware multi-hop paths, when the number of such paths is larger; the proposed scheme can tolerate higher node compromised probability. Due to the selection process of random path, the selected paths may intersect, that is, some nodes appear in more than one path from a source node towards to storage node and thus, the security performance worsens. This result verifies the effectiveness of the proposed idea.

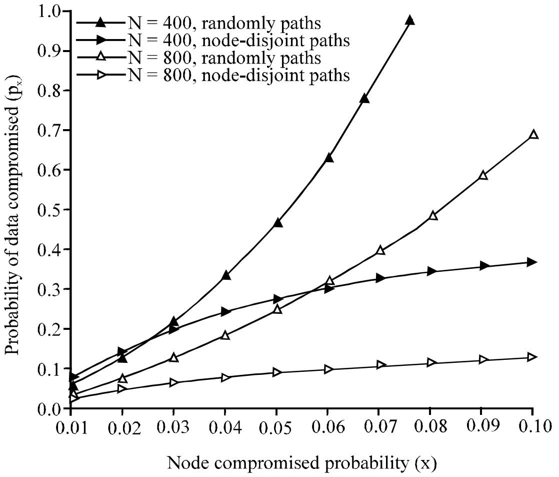

Fig. 1: p_x as a function of *x* for different node density and routing strategy

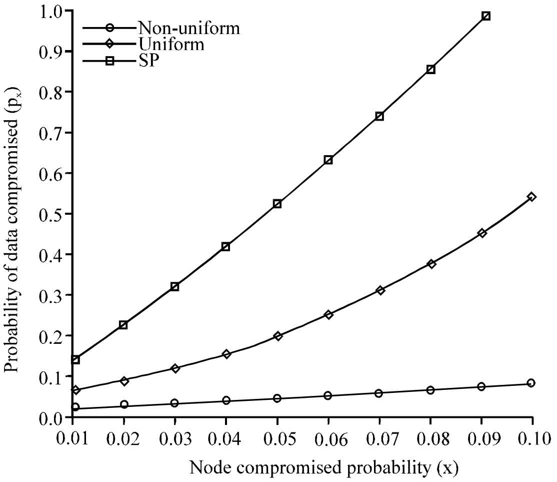

Fig. 2: p_x as a function of *x* for different data allocation scheme

Figure 2 presents the data compromise probability from another angle, where p_x is a function of node compromise probability x for different data share distribution scheme. The uniform allocation can be regarded as $f_j = 1/m$ for all paths and single path (SP) scheme is to send all shares through one path. Based on Fig. 2, it can be concluded that the non-uniform allocation applied in the proposed scheme outperform uniform scheme and SP scheme in terms of lower probability of data compromised. Such as if x is 0.06, then p_x for the proposed scheme, uniform scheme and SP scheme is 0.05, 0.25 and 0.6, respectively. The proposed scheme improves 5 times and 12 times over uniform scheme and SP scheme, respectively. It can further conclude that the selection of f_j has major effects on security performance. In the uniform scheme, long paths may be assigned with equally size of shares and lead to higher probability of data compromised. Moreover, the results proved again that multipath transmission is preferred over SP scheme when security is a major concern.

Figure 3 presents the probability of data compromised by varying the value of (n, k) and show data compromise probability p_x for different node compromised probability x. Based on this figure, it can be conclude that p_x is decreased by increasing both n and k, the network can tolerant faulty paths from t = 1 to 4 given m node-disjoint paths. More importantly, it provides a nice property of flexibility that a predefined threshold of p_x can be guaranteed by choosing an appropriate (n, k). For example, given a system threshold $p_x = 0.4$, with node compromised probability from 0.01 to 0.09, only (17, 9), (13, 7) satisfied the requirement, given $p_x = 0.1$, only (17, 9) satisfied the conditions when the node compromised probability lower than 0.05.

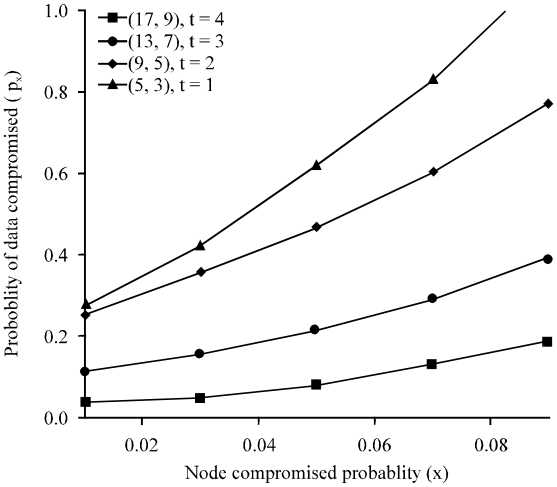

Fig. 3: p_x as a function of *x* for (17, 9), (13, 7), (9, 5), (5, 3) RS coding schemes.

A comparison is made between the proposed scheme and H-SPREAD (Lou and Kwon, 2006); First, consider the circumstance that there is no data modification happen in the network. Define the robustness as the probability of data not compromised due to r compromised nodes, denoted as R_1, obviously, $R_1 = 1\text{-}p_x$. Fig. 4a shows R as a function of r for the proposed scheme and H-SPREAD. Based on this figure, it can be conclude that the proposed scheme outperforms H-SPREAD with better robustness as r increases. In H-SPREAD, the author attempts to find multiple node-disjoint paths for both security and reliability. As a result, the number of node-disjoint paths is small. Besides, each path is sent to equivalent number of symbols leading to the poor performance. An example of these results is that when r is 100, 200, 300, the robustness of H-SPREAD is 0.575, 0.175 and 0.022, respectively. When r up to 350, the robustness of the proposed scheme and H-SPREAD is 055 and 0, respectively, obviously, the proposed scheme significant improves the robustness of the network. Further

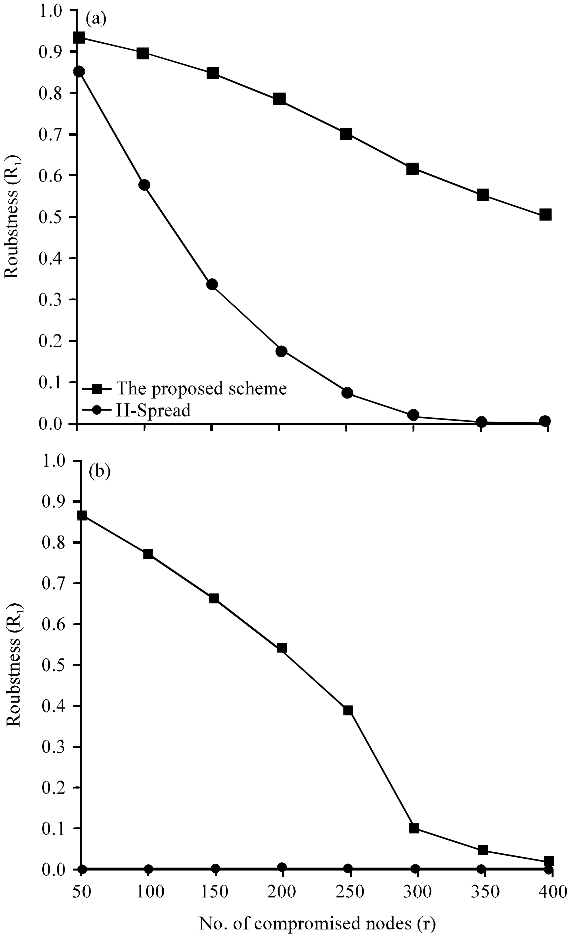

Fig. 4: Comparison (a) robustness and (b) reliability of the proposed scheme with H-SPREAD

conclusion can be made that the selection of node-disjoint paths and non-uniform data allocation as well as redundancy has major effects on robustness in the proposed scheme.

Consider another circumstance that the adversary compromises r sensor nodes and they can further modify existing data and/or inject fake data into compromised sensors. Define reliability as the ratio of filtering bogus message, denoted as R_2. Figure 4b plots R_2 as a function of r for the proposed scheme and H-SPREAD. Based on this figure, it is observed that the reliability of the proposed scheme significantly improved over H-SPREAD. Actually, in H-SPREAD, it cannot address a number of important problems, such as, the authenticity of sensed data, the possibility that adversary modifies in any data found in sensor nodes. Once the sensor node is captured, the cryptographic keys as well as the data were exposed. They can easily insert bogus sensor readings or change the processing results and then use these keys to authenticate forged information. Thus, H-SPREAD fails to filter faked messages. In the proposed scheme, RS coding scheme which can tolerant at most terrors, where t = (n-k)/2. Therefore, it can achieve higher reliability. However, it has to point out that when r exceeded in 250, the reliability of the proposed scheme drops dramatically, after *r* up to 400, the reliability of the proposed scheme has no benefits over existing schemes. In this case, it can be explained that with the more compromised nodes in the networks, the more faulty paths exists, if the number of faulty path more than t, it cannot use the majority rule to filter out bad parity codes. However, when that happens, they are telltale signs indicate massive nodes invalid and should exclude out of the network.

DISCUSSION

The concept of multi-path routing dates back to 1970s, when it was initially proposed to spread the traffic for the purpose of load balancing and throughput enhancement (Maxemchuk, 1975). Later on, one of its sub-classes, path-disjoint multi-path routing, has attracted a lot of attention in wireless sensor networks due to its robustness in combating security issues. Some examples include the SMR (Lee and Gerla, 2007), DSR (Johnson *et al*., 1999), and AOMDV (Marina and Das, 2001) and AODMV (Ye *et al*., 2003).

The second category includes recent work that explicitly considers security metrics in constructing routes. Specifically, the SPREAD algorithm by Lou *et al.* (2004) attempts to find multiple most secure and node disjoint paths. The security of a path is defined as the likelihood of node compromise along that path and is labelled as the weight in path selection. A modified Dijkstra algorithm is used to iteratively find the top-k most secure node-disjoint paths. The H-SPREAD algorithm (Lou and Kwon, 2006) improves upon SPREAD by simultaneously accounting for both security and reliability requirements.

The work by Yang *et al.* (2005) considers the report fabrication attacks launched by compromised nodes. The work by Ren *et al.* (2006) further considers selective forwarding attacks, whereby a compromised node selectively drops packets to jeopardize data availability. Both works are based on a similar cryptographic method: the secret keys used by sensor nodes are specific to their geographic locations, which limits the impact of a compromised node.

Most of above mentioned works relying on a cryptographic method for resolving the node capture attacks. As a result, these approaches are no longer valid if the adversary randomly compromise or jam nodes. This is because once the adversary captures a sensor node, the credential and the encryption algorithm will be disclosed, even they can limit the impact of a compromised node within a local area. Instead of relying on a cryptographic method for resolving the issue, this work mainly exploits the routing functionality of the network to reduce the chance that the adversary can acquire a packet in the first place. Besides, by taking the advantage of the fact that different paths have different probabilities of being compromised or becoming faulty. Therefore, different amounts of symbols are sent through paths of different lengths. By doing so, the adversary has to compromise a k out of n sensors to recover the original data. Besides, 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. The experiment results are well support with the analysis and verify the effectiveness of the proposed scheme.

CONCLUSIONS

This study has presented an efficient in-network sensor data-delivering scheme in distributed wireless sensor networks. As is shown above, the presence of a powerful mobile adversary raises many challenges. The conventional view of security based on cryptography and authentication alone is not sufficient to provide a complete solution for developing secure and dependable sensor data delivery due to the unique characteristics and novel misbehaviours encountered in distributed sensor networks. This study investigates the first attempt to introduce RS code scheme and multipath routing protocol to add an additional support for an enhanced security solution. Analysis and simulation results show that proposed techniques significant improvement the data survival over existing scheme.

ACKNOWLEDGMENTS

This study is partially supported by National Basic Research Program of China (973 Program) under Grant No. 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), 60973113 (2010.1-2012.12, Hunan University), 61073191 (2011.01-2013.12, Hunan University) and 61070196 (2011.01-2013.12, Hunan University).

REFERENCES

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

Goodson, G.R., J.J. Wylie, G.R. Ganger and M.K. Reiter, 2004. Efficient byzantine-tolerant erasure-coded storage. Proceedings of the International Conference on Dependable Systems and Networks, (DSN'04), IEEE Computer Society, Washington, DC, USA., pp: 135-144.

Johnson, D.B., D.A. Maltz and J. Broch, 1999. DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. In: In Ad Hoc Networking, Perkins, C.E. (Ed.). Addison-Wesley, USA., pp: 139-172.

Lee, S.J. and M. Gerla, 2007. Split multipath routing with maximally disjoint paths in ad-hoc networks. Proceedings of the ICC Conference, June 11-14, IEEE., pp: 3201-3205.

Lin, S. and D.J. Costello Jr., 2004. Error Control Coding: Fundamentals and Applications. 2nd Edn., Prentice Hall, Englewood Cliffs, New Jersey.

Lou, W. and Y. Fang, 2001. A multipath routing approach for secure data delivery. Proceedings of the Communications for Network-Centric Operations: Creating the Information Force, (MILCOM’01), IEEE., pp: 1467-1473.

Lou, W., W. Liu and F. Yuguang, 2004. SPREAD: Enhancing data confidentiality in mobile ad hoc networks. Proceedings of 23rd AnnualJoint Conference of the IEEE Computer and Communications Societie, March 7-11, Hong Kong, China, pp: 2404-2413.

Lou, W. and Y. Kwon, 2006. H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transact. Vehicular Technol., 55: 1320-1330.

Marina, M.K. and S.R. Das, 2001. On-demand multi path distance vector routing in ad hoc networks. Proceedings of the 9th International Conference on Network Protocols, Nov. 11-14, Washington, DC., USA., pp: 14-23.

Maxemchuk, N.F., 1975. Dispersity routing. Proc. IEEE ICC., 41: 10-13.

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.

Papadimitratos, P. and Z.J. Haas, 2006. Secure data transmission in mobile Ad-Hoc networks. IEEE J. Selected Areas Comm., 24: 343-356.

Ren, K., W. Lou and Y. Zhang, 2006. LEDS: Providing location-aware end-to-end data security in wireless sensor networks. Proceedings of the IEEE INFOCOM Conference, April 23-29, IEEE., pp: 2584-2595.

Ren, H., X. Sun, Z. Ruan and B. Wang, 2011. An efficient scheme against node capture attacks using secure pairwise key for sensor networks. Inform. Technol. J., 10: 71-79.

Ruan, Z., X. Sun, W. Liang, D. Sun and Z. Xia, 2010. CADS: Co-operative anti-fraud data storage scheme for unattended wireless sensor networks. Inform. Technol. J., 9: 1361-1368.

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

Wang, B., X. Sun, Z. Ruan and H. Ren, 2011. Multi-mark: multiple watermarking method for privacy data protection in wireless sensor networks. Inform. Technol. J., 10: 833-840.

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.

Yang, H., F. Ye, Y. Yuan, S. Lu and W. Arbaugh, 2005. Toward resilient security in wireless sensor networks. Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing, May 25-28, USA., pp: 34-45.

Ye, Z., V. Krishnamurthy and S.K. Tripathi, 2003. A framework for reliable routing in mobile ad hoc networks. Proc. IEEE INFOCOM., 1: 270-280.