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 (4): 740-748, 2010
ISSN 1812-5638

Multiple Hash Sub-Chains: Authentication for the Hierarchical Sensor Networks

[1]Ang Gao, [1]Wei Wei and [2]Xiangrong Xiao
[1]School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, China
[2]School of Computer and Communication, Hunan University, Changsha, 410082, China

Abstract: Wireless Sensor Networks (WSNs) are often deployed in hostile environments, thus being subjected to great security risks. Secure authentication between the two participating entities is of typical defense against data modified and fabricated by an adversary. In this study, considering environment and dynamic topology having a significant impact on the communication radius of sensor, we proposed a secure Multi-hop authentication scheme: the data message source is verified with keys derived from multiple one-way hash sub-chains related to communication radius of node, while offering greater resilience against node compromised by designing the hash chain length which guarantees that sub-chains are picked with the low probability of overlap between two or more sensors. Compared to existing solution, the proposed method greatly alleviates extra memory space taken and lower energy consumption extends the network lifetime benefiting from the distributed strategy.

Key words: Wireless sensor networks, hash chain, hierarchical authentication, different communication ranges, internal attack

INTRODUCTION

In Wireless Sensor Networks (WSNs), sensors are deployed in open environment of lacking infrastructure, nodes normally rely on batteries to provide energy and are more vulnerable to be captured, compromised, hijacked and eavesdropped by anyone who has the proper wireless equipment. The confidential information about security mechanisms that rely on authentication or encryption may be invalid and the adversary can use these hijacked nodes to disrupt the network. Therefore, it is imperative that wireless networks are able to identify other legitimate nodes on the network in order to allow both authenticated entities to engage in a secure communication.

Some research (Xiao *et al*., 2009; Cao *et al*., 2007) works have been conducted on authentication in WSNs. Deng *et al*. (2005) proposed an authenticating scheme for defending against path-based DoS attacks. Authenticating keys are picked from key chains when transmitting data messages each time. If sending excessive packets, a large size of key chain is required to establish in advance and results in inadequate memory storage. μTESLA is a security protocol for broadcasting authentication with a one way hash chain (Perrig *et al*., 2002). However, to accomplish the key initialization and synchronization, μTESLA requires the distribution of some bootstrapping material via unicast communication, which is not efficient for a large scale sensor network.

Several schemes have been proposed to extend the μTESLA with multiple-level key instead of single-level key, to improve privacy and performance, Liu and Ning (2003) extend μTESLA to a two-level key ring structure, which serves as a foundation for the work of Tany *et al*. (2008), it is proposed that a Multi-hop authentication scheme with multiple one-way key chains, according to nodes hop distance to the base station. Deng *et al*. (2005) proposed an authenticating scheme for defending against path-based DoS attacks; authenticating keys are picked from key chains when transmitting data messages each time. But, the scheme (Tany *et al*., 2008) is a centralized version, not only the overhead in base station is easy to be a bottleneck, but also redundant neighbors and grouping packets with broadcast transmission, consume much energy.

Moreover, WSNs may occur unidirectional links related to sensor's energy. Though, the energy of each sensor is same during WSNs initialization, it varies finally under the influence of environment and dynamic topology, which fluctuates the power of sensor. Based on the theory (Li-Min and Gui-Ming, 2006) about power related to the communication range, the power of a sensor is proportioned to its exponential communication range, it means that the larger transmission radius involves a higher number of neighbors competing to access the medium; therefore each contract node has a longer contention delay for packet transmissions. On the other hand, a smaller communication ranges involves a fewer

Corresponding Author: Ang Gao, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, China Tel: 86-29-82664597

umber of neighbors are insufficient to maintain network connectivity. Therefore, the neighbor's number is significant for extending the network lifetime. Numerous protocols are proposed to discover neighbor (cluster) sensors, such as ReInForM (Deb *et al*., 2003), LEACH (Heinzelman *et al*., 2002), GAF (Xu *et al*., 2001), TopDisc (Deb *et al*., 2002) and several schemes (Kleinrock and Silvester, 1978), (Takagi and Kleinrock, 1984) have been proposed to determine the number of neighbors. But, all of them are assumed to be the same radio ranges based disc graph. Hou and Li (1986) considered different transmission range of node individually and obtained the magic numbers six and eight. Thai and Du (2006) proposed a maximum number of independent neighbors algorithm in disk graphs with bidirectional links concern of the different transmission ranges of all nodes, but it requires the distribution of neighbors to be rigorous, which is unsuitable for practical application. Moreover, though a maximum number of independent neighbors can be figured out, yet how to inquire these neighbors is not discussed. As a result, although all neighbors through the flood to a communication node within the scope can be found, yet it will result a larger communication overhead.

In this study, we first solve the neighbor discovery during classifying neighbors of each node, consequently, less neighbor nodes can be discovered according to the different communication ranges to the node by sending a few query messages instead of broadcasting messages. after hierarchizing neighbours, we introduce a multiple key sub-chains authentication method which extends centralized algorithm by Tany *et al*. (2008) to a distributed algorithm by generating the hash sub-chain, whose size is associated with the number of neighbors instead of frequency of packet transmission (Deng *et al*., 2005).

NETWORK MODEL DEPICTION

To the best of our knowledge, most of existing secure schemes are performed consideration of the same radio ranges. Yet, the wireless communication range is related to energy, which is generally different in each sensor due to impact of mountain, building tamper and bad climate environment, though every node has the same energy in initialization, varied routing paths incur different energy consumptions which make each node exist in different communication radius finally. Considering, the influences mentioned above, the network model is based on the following assumptions:

- Every node has the different transmission radius based on its power
- The area of the network can be approximated as a square
- Few nodes are mobile

MULTIPLE ONE-WAY KEY SUB-CHAINS MESSAGE VERIFICATION ALGORITHM (MKSV)

Neighbor discovery and initial grouping: Li-Min and Gui-Ming (2006) proposed the relationship between power E and communication range of neighbor r, as shown in Eq. 1, where the hop number h is generally set as three, that is the number of the message passed with the query angle α_i which is specified randomly by query node. We conducted this study to develop a distributed grouping scheme which is similar to token-ring mode. A grouping e(R) which a neighbor belongs to is defined by the Eq. 3 and the transmission time T(e) of packet is defined by the Eq. 2, where independent variable R is real radio range of neighbor, the minimal radio range is denoted by R_{min} and c denotes the transmission speed.

$$E(r) = k(2r)^h \qquad (2 < h < 4) \tag{1}$$

$$T(e) = eR_{min}/c \tag{2}$$

$$e(R) = \lceil R/R_{min} \rceil \tag{3}$$

The process of neighbor discovery is shown in Fig. 1a. The passed angle θ of query message for neighbor is derived by the Eq. 4, where i denotes query time. The incline angle β can be calculated as Eq. 5.

One node O at an angle of α_1 degrees sends a token message, which appends a radio range R_1, a time stamp TAP of current node O, transmission time T(e), minimum radio range R_{min} and ID, When node A receives it, $T=TAP_A-TAP_0$ is computed in order to be compared with T(e), if T is unequal to T(e), the token message is forwarded at the angle of α_1 degrees. If T is equal to T(e), the node A then verified whether $E(R_A)$ which is by (1) is equal to $E(eR_{min})$, if they are equal, the neighbor A is matched for node O, it sends a feedback message with ID_A to the node O, subsequently, T(e) and ID is updated by T(1) and ID_A, the query message is forwarded to next node B at an angle of θ_1 degrees. Otherwise, the same operation (only forwarding) is performed as the matched case with the exception that the feedback message is unsent. In this way, the query message is passed on until it returns the initiative node A. Next, in second round, the same operation as the first round is executed, another token

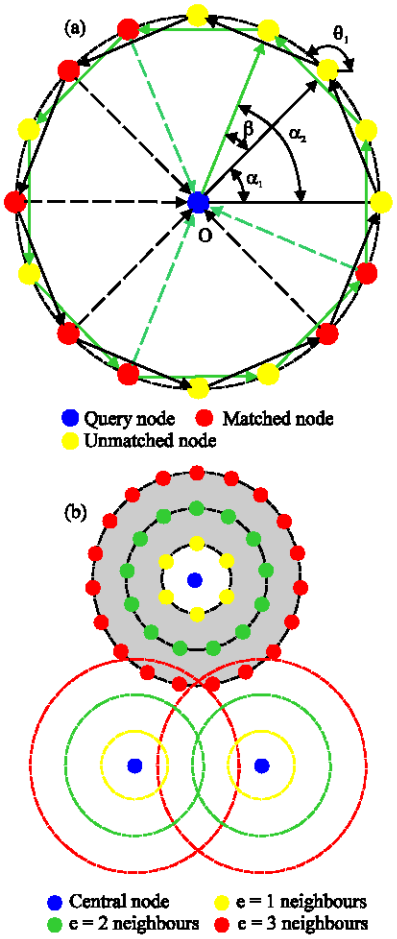

Fig. 1: Neighbour discovery and initial grouping. (a) neighbour nodes discovery, (b) the torus hierarchy of neighbour nodes

message is sent by query node at angle of α_1 degrees increased, where, α_i-α_{i-1} (k = 1, 2, 3…n). Finally, after n rounds queries are completed, matched neighbors may be disclosed in multiple cirques of radius R_i with center O when, sensors are distributed uniformity, different level neighbors grouping is illustrated in Fig. 1b.

$$\theta_n = 90° + \alpha_i + (2n-1)\beta \qquad (\alpha_i - \alpha_{i-1} \le 2k\beta) \tag{4}$$

$$\sin\beta = 1/2e \tag{5}$$

Key pre-distribution: A hash chain consists of multiple sequence values K_0, K_1, K_2… K_n, Subsequent values K_i, for I: n>i = 0, are computed as $K_i = H(K_i+1)$ where, H is a hash function. Furthermore, the initial element K_n is employed for the hash chain seed and assumed to be randomly and uniformly selected from n-bit binary string. One-way property of hash function H means, given independent variable x, it is easy to compute H(x), whereas, invertible function H(x) is hard or unfeasible on average to seek x.

After grouping neighbors, firstly, the base station generates S different level hash chains with length of L+1 with S independent random seeds. The ith sequence value from eth layer hash chain is denoted as K^e_i. In initialization, correspondence layer neighbors are deployed initially with K^1_0, K^2_0,.., K^e_0 which central node received from the base station. Through the advantages of ring hierarchical structure, key pre-distribution can be completed via a few messages passed on as the token-ring instead of broadcasting to all members of the whole networks. In authentication phase, each node has a well-known hash function H on it. Assume, H is one-way and thus it is intractable to invert. Second, the ith source node which senses the external data is distributed a key subset of multiple hash chains from the base station in secure communication (e.g., Diffie-Hellman key exchange (Diffie and Hellman,1976)), which is denoted as the $ring_i = \{C^1_k, C^2_k \ldots C^e_k\}$, the element C^e_k in set indicates that k hash keys elements are selected randomly from e^{th} layer chain, called a hash sub-chain. Each intermediate node maintains a key set that are distributed, called key pool, with the same size with the layer number. Initially, key pool is set to $\{K^1_0, K^2_0, .., K^e_0\}$ with discussed above scheme. The detailed steps are shown in Algorithm 1 and Fig. 2 (show as dashed frame, sub-chains are selected continuously. In practice, they can be picked discretely).

Algorithm 1: Neighbour discovery and initial grouping

Input: $\alpha_i R_{min}$
Output: matched nodes
Body:
1: O: compute T(e), β and Generate TAP_O
2: while (α_i-$\alpha_{i-1} \le 2k\beta$) then
3: O :M← MSG||e||TAP_O||T(e)||R_{min}||ID_O
4: $O \xrightarrow{\alpha_i} *$:M
5: A (one of nodes that receive M):
6: while ($ID \neq ID_A$) do
7: If (TAP_A- TAP_O = T(e)) then
8: $TAP_O \leftarrow TAP_A$
9: A:Compute $E(R_A)$ and $E(eR_{min})$
10: If ($E(R_A) = E(eR_{min})$) then
11: A→O :ID_A
12: End if
13: Compute T(1) and $\hat{e}_i$
14: T(e)←T(1)
15: ID←ID_A
16: $A \xrightarrow{\theta_i} *$:M
17: else
18: A: Drop M
19: End if
20: End while
21: O: i←i+1
22: End while

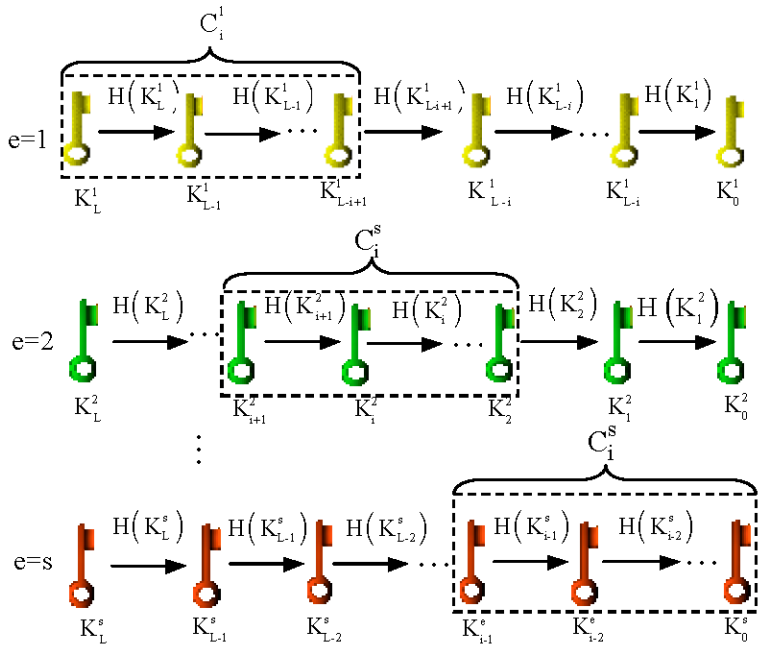

Fig. 2: Hash sub-chain keys pre-distribution (show as dashed lines frame)

Choosing the layer key (K^e_i): It is assumed that the neighbors have been grouped using proposed method in the last section and a routing path has been established along source node S to destination node D using existed routing algorithm. S has n neighbors which denote N_1, N_2, …N_n in different layers along path SD, If considering directional link, any node among N_1, N_2, …N_n can be selected for next hop node, but after hierarchizing neighbours learns differences in power E among neighbours, it can choose the neighbour N_e which has the greatest power E in the layer e as the next hop node. At the same time, the ith key K^e_i in corresponding layer is determined for the authentication. Taking into account the energy balance, when energy of N_e descends below a threshold (v) that assures bidirectional links between source and its neighbours, the other level neighbour with the inferior greatest E in the layer is selected as the next hop node, so a new corresponding layer key is employed for authentication. Finally, all level neighbours likely may be served as an inter-mediate node for forwarding packet along the path SD.

Multiple One-way Key Sub-chains Message Verification (MKSV): When, one node A want to send a data message M to B, it picks a K^x_i randomly from ith sub-chain C^x_i in ring according to the layer x where, the next hop node B may locate and this is determined by above discussed layer key choosing scheme. It then sends the index i of K^x_i to B, as B receives it. assuming B has a previous key K^x_j in its key pool, if i is not greater than j, B obtains the hash element $(K^x_i)'$ by performing (j-i) times hash computation for K^x_i until j is reduced to i. B then informs A that the message appending the MAC which is computed with $H(M\|K^x_i)'$ can be sent after receiving it, B then may verify whether, $H(M\|(K^x_i)')$ is identical with MAC or not, equality between them indicates that M is not modified by the malicious node during transmission. At the same time, the previous stored key K^x_j in memory is replaced by $(K^x_i)'$. Otherwise, the message may be suspected of modification and should be discarded. if i is greater than j, B sends j to A which obtains the hash element $(K^x_j)'$ by performing (i-j) times hash computations for K^x_j until i is reduced to j, subsequently, A sends the message appending the MAC which is computed with $H(M\|(K^x_i)')$ to B, after receiving it, B verifies whether $H(M\|K^x_i)$ is equal to MAC or not, if both are the same, the message is authorized and K^x_j in A is replaced by $(K^x_j)'$. Otherwise it is discarded. The detailed steps are shown in Algorithm 2.

Algorithm 2: Bob(B) verifying message from Alice(A)

Input: data message M
Output: whether M is authorized or not

Body:
1: A selects a K^x_i from ith sub-chain C^x_i in the ring according to layer key choosing scheme
2: A→B: i
3: B: receive i
4: if (i = j) then
5: $B:(K^x_i)' \leftarrow H(\underbrace{...H(K^x_j)}_{j-i})$

Algorithm 2: Continued

6: A→B: $M\|H(M\|(K_j^x)')$

7: if $\left(H\left(M\|\left(K_i^x\right)'\right)=H\left(M\|K_i^x\right)\right)$ then

8: B: accept M

9: Else

10: B: drop M

11: End if

12: Else if (i>j) then

13: B→A: j

14: A: receive j

15: $A:\left(K_j^x\right)' \leftarrow \underbrace{H\left(...H\left(K_i^x\right)\right)}_{i-j}$

16: A→B:$M\|H(M\|(K_j^x)')$

17: If $\left(H\left(M\|K_j^x\right)=H\left(M\|\left(K_j^x\right)'\right)\right)$ then

18: B: accept M

19: Else

20: B: drop M

21: End if

22: End if

SECURITY ANALYSIS

Internal attack: Attacks can be categorized into external and internal attacks in terms of adversary's venue. An external attack is generated by malicious nodes that be excluded from the network. An internal attack is launched by compromised or hijacked nodes that have formerly legitimate identity. Therefore, an internal attack is much more difficult to prevent, comparing with an external attack. Due to the confidential information about security mechanisms, that rely on authentication or encryption may be learned by node. Similarly, our scheme can be vulnerable to the internal attack in certain degree. The success likelihood is discussed below in detail.

Definition: One-point eroded for hash chain means hash chain is divided into A segment and B segment logically with a certain location d as the boundary, due to d in hash chain S_L^e is revealed resulting from successful attacks for nodes with inadequate physical protection. According to the one way feature of hash chain, the down-stream segment A of d is disclosed entirely, which is called eroded segment. On the other hand, the up-stream segment B of d keeps in secret, as shown in Fig. 3.

Theorem: The S_L is assumed to be a one way hash chain, due to the eroded position d is randomly and equiprobably located in any key from the chain, the probability P_A that corrosion successfully appears in the hash chain can be computed as Eq. 6, when at least one of multiple attack positions is successfully broken:

$$P_A = \frac{n_a}{L} \quad \left(n_a = 0,1,2,...,L\right) \tag{6}$$

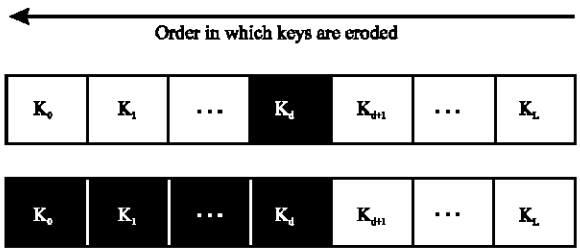

Fig. 3: One point eroded in hash chain

where, L denotes the length of hash chain and n_a is the number of attack positions.

The location of chain corrosion relies on the optimum strategy for an attacker, that means n_a is generated randomly and uncontrolled for WSNs. So, the hash chain L has a direct impact on the proportion P_A-increasing L leads less keys leakage and decreasing L has the opposite effect. On the other hand, in order to drop the eroded proportion every level sub-chain should be selected in the up-stream segment of the whole chain, which increases the probability of overlap among key elements in sub-chains. Accordingly, because the smaller chain length L results from overlap sub-chains with a closer distance each other, the proportion of segment eroded rises and the eroded speed is more rapid. It costs fewer times of hash computation for an attacker to obtain keys. In order to address these issues, the length of chain L has to be designed to be as medium-scale as possible. Based on the scheme (Laurent and Gligor, 2002), the probability of segment eroded occurring and simultaneously any two sub-chains with an overlap of at least one key in single hash chain, can be shown as below formula and Fig. 4, where, l is the length of the hash sub-chain.

$$P_e = \begin{cases} \dfrac{n_a}{L} - \dfrac{n_a\left((L-1)!\right)^2}{L^2(L-2l)!(L-1)!} & (L \geq 2l) \\ \dfrac{n_a}{L} & (1 \leq L < 2l) \end{cases}$$

Designing of the length: In order to address the tradeoff between corrosion for the hash chain and the overlap of sub-chains, we can search for an optimal chain length L that satisfies security requirement. Given the sub-chain length l and layer e, the below relationship must be satisfied:

$$\underset{l \in \Theta}{SUP}\left(P(l)\right) \leq \alpha$$

where, Θ denotes the alteration range for L, α denotes a tiny probability of hash chain corrosion occurring and

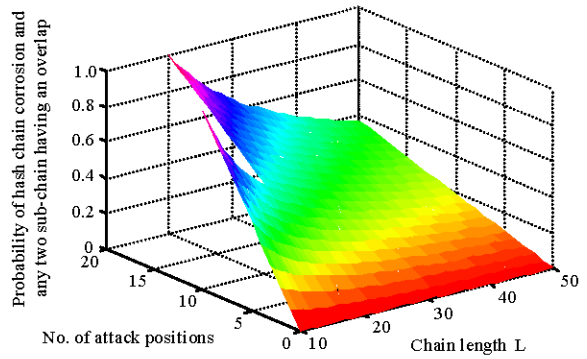

Fig. 4: The probability of segment eroded occurring and simultaneously any two sub-chains with an overlap of at least one key in single hash chain, when, l = 10, 10≤L≤50

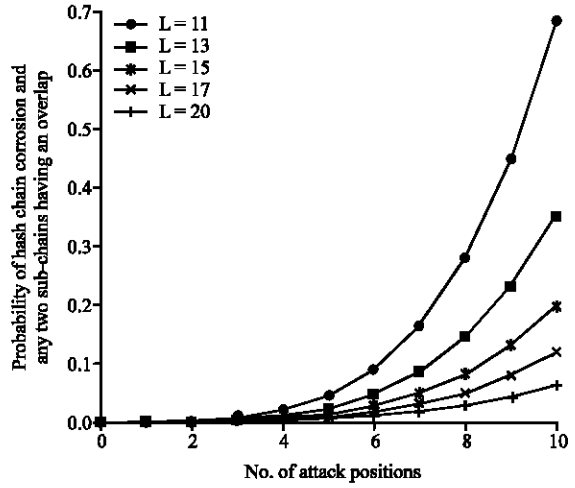

Fig. 5: The probability comparison of corrosion occurring at all layers e with different lengths L of the chain (l = 10, e = 4)

simultaneously any two sub-chains having an overlap of at least one key, $\sup_{l\in\Theta}(P(l))$ is upper boundaries. Figure 5 shows the probability comparison of hash chain corrosion occurrence and simultaneously any two sub-chains with an overlap of at all level chains with different chain length L (L is increased with values as are 11, 13, 15, 17 and 20, respectively), under the assumptions given α = 0.1. It is believed that the security improvement in increase of chain length L outweighs the number n_a of attack positions. Consequently, in order to keep the probabilities varying from 0.01 to 0.1, it would be best that the dereferencing of L is bigger than 20 based on the curve tendency of Fig. 5.

PERFORMANCE EVALUATION

Memory comparison: In terms of the results (Tany *et al*., 2008), the maximum packet size in TinyOS is 128 bytes. We utilize a hash function such as SHA-1 to assign keys. The default size of hash output in SHA-1 is 20 bytes (Eastlake and Jones, 2001), which is used for authentication segment. The key size for performing one hash or MAC computation using RC5 (Rivest, 1994) block cipher is denoted as k. On accounting of the tradeoff between security and resource availability, the key size k has to be designed to be as medium-scale as possible.

Moreover, in Berkeley Mica2 Mote, the TR1000 and CC1000 types of chip are utilized generally, where the communications ranges of sensor vary from 100 to 300 m and 500 to1000 m, respectively and the number of layer e for neighbors can't exceed 4 in general. As a result, the additional memory space occupied by intermediate nodes is:

$$W_{int}(k) = k \times e + 20$$

The comparison of extra memory space per node (except for sensing nodes) results, using the MKSV scheme and multiple one-way key chains verification (MKCV) scheme, are shown in Fig. 6a. The results show that the MKSV scheme proposed has less extra memory space than original MKCV scheme when only one layer existing. when e is increased to 2, the key size k is lowered to 18bytes in order to get less extra memory space, thus the similar results are found in Fig. 6a when, e = 3, k<9bytes and e = 4, k<5bytes. As for the sensing source node, whose function is almost the same as the base station in MKCV scheme, because it generates multiple hash sub-chains and picks an initial key randomly from key pool to verify data message. Consequently, the extra memory space in sensing source node in our scheme can be defined in below formula:

$$W_{sense}(k) = (k \times 1 + 20) \times e$$

We compare the extra memory space taken of sensing nodes in our scheme with the base station in MKCV scheme. The results show in Fig. 6b that the sensing source node has less extra memory space than the base station in MKCV scheme, because the length of sub-chain that is divided in our scheme is always shorter than that of chain in MKCV scheme.

Comparison of energy consumption in authentication phase: We use the results presented in (Ye *et al*., 2004) that sensor consumes ε_s =16.25 and ε_r=12.5 μJ bit^{-1} to run

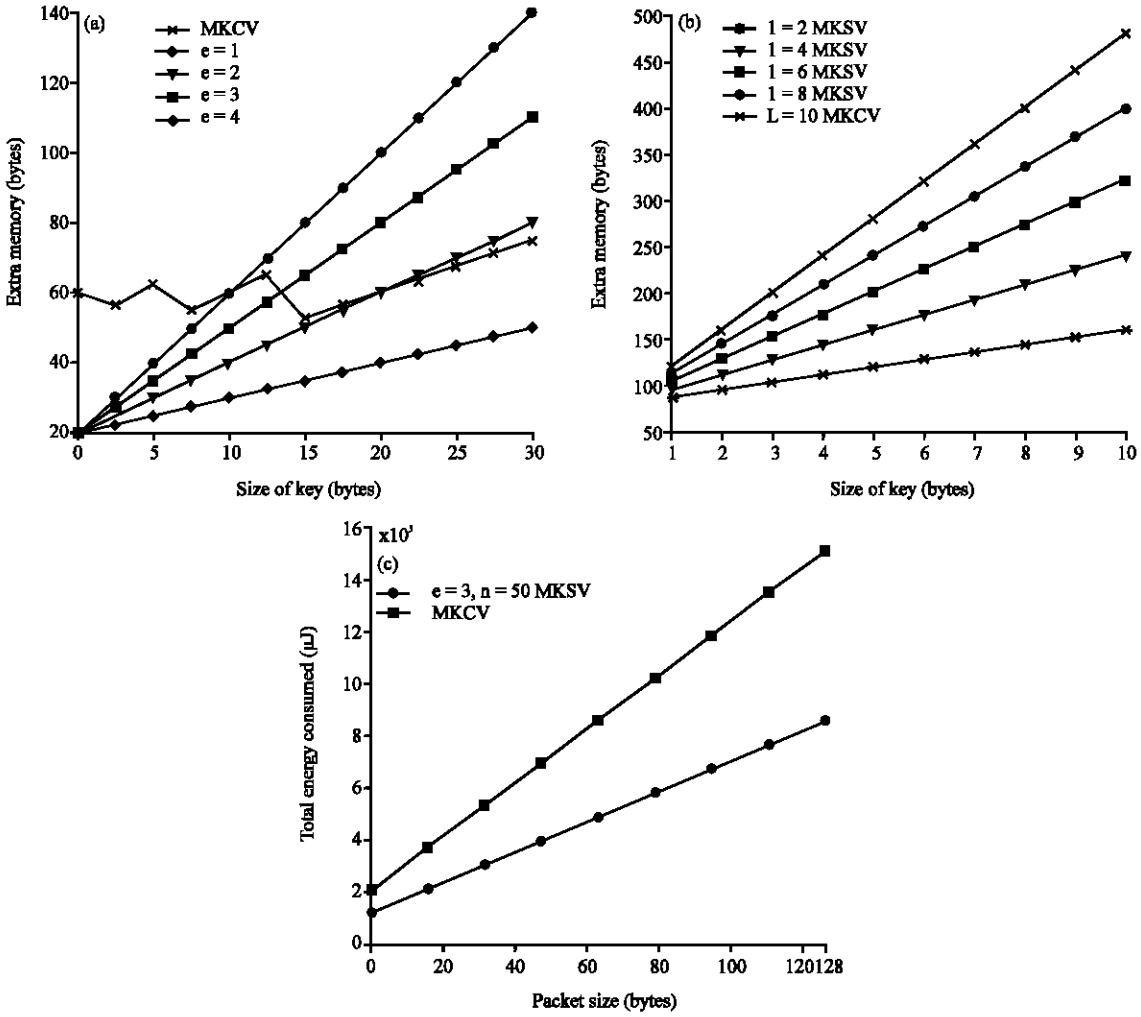

Fig. 6: Extra memory and total energy consumption comparison. (a) Extra memory comparison of forward node with the MKSV and proposed scheme, (b) Extra memory comparison with MKSV in sensing source node and MKCV in base station and (c) The total energy consumption comparison by neighbors during authentication phase with MKSV and MKCV

the transmitter and receiver circuitry using Berkeley Mica2 Motes. The energy consumption for performing one hash or MAC computation using RC5 (Rivest, 1994) block cipher is ε_h = 15 µJ and takes about 0.5 msec. The size m of packet, from which 20 bytes are truncated for generating MAC using SHA-1 Hash algorithm, is not larger than 128 bytes in a MICA2 sensor node. Sensor nodes are densely and uniformly deployed in a flat area with 2.5 nodes m^{-1} and 25 nodes m^{-2}. Thus, the total energy consumed by neighbors during authentication phase is given by Eq. 7, where e is denoted as the number of hierarchical neighbors after using our scheme:

$$E(m) = \left(\left((m + 20) \times 8 \times (e_s + e_r)/2 \right) + e_h \right) \times e \qquad (m \le 128) \quad (7)$$

We compared the total communication overhead (in µJ) of WSNs during authentication phase incurred of our scheme with that of MKCV (Tany *et al*., 2008) under the assumption that the number n of hierarchical neighbors is 50 after using our scheme of hierarchical neighbors and layer number e is 3. Figure 6c shows that, as packet size m increases, both the communication overheads of our scheme and MKCV increase, but the total energy consumption of our scheme has always lower cost than that of MKCV, because choosed neighbors of our scheme by taking advantage of ring hierarchical structure are far less than that of MKCV, which has too many successive neighbors for one central node resulting in the higher energy consumption.

CONCLUSION AND FUTURE WORK

In this study, We have developed a secure authentication scheme for the different radio ranges sensor with multiple one-way sub-chains, The key idea is hierarchical neighbors according to neighbors radio range to the node and authentication is to be achieved with keys derived from multiple low-overlap hash sub-chains, we employ torus topology similar to token-ring in neighbors grouped discovery phase and key pre-distribution phase to reduce the extra memory space and energy consumption, we further validated the eroded probability in Hash chains to alleviate jeopardy from internal attack launched by an adversary. We achieved exceptional low eroded probabilities of Hash chains by length of chain design. However, the scheme proposed only adapts to 2-dimensinal torus environment, when sensors are deployed into an area not so even, the network topology should be a 3-dimensinal cirque-tyre instead of torus, as our future work we would like to extend the scheme for torus to cirque-tyre scene.

ACKNOWLEDGMENTS

This work was partially or fully sponsored by National Natural Science Foundation of P.R. China (NSFC No. 30973128, 60973113 and 60873198) and National Basic Research Program of P.R. China (973 No. 2006CB303000 and 2009CB326202), authors would like to thank Wei Wei for helpful discussions and insightful comments. He reviewed the draft of the study and made further modifications that improved the quality of the study. Xiangrong Xiao devoted herself to designing some graphs and other art works in this study. We also thank the anonymous reviewers for their insightful and valuable hints.

REFERENCES

Cao, C.J., C. Yang, X.H. Li, Y.B. Guo and J.F. Ma, 2007. Perfect forward secrecy of authentication and key exchange protocols in three versions of WAPI. Inform. Technol. J., 6: 1108-1113.

Deb, B., S. Bhatnagar and B. Nath, 2002. A topology discovery algorithm for sensor networks with applications to network management. Proceedings of the IEEE CAS Workshop on Wireless Communications and Networking, September 2002, Pasadena, USA., pp: 1-4.

Deb, B., S. Bhatnagar and B. Nath, 2003. ReInForM: Reliable information forwarding using multiple paths in sensor networks. Proceedings of the 28th Annual IEEE Conference on Local Computer Network, Oct. 20-24, Germany, pp: 406-406.

Deng, J., R. Han and S. Mishra, 2005. Defending against path-based DoS attacks in wireless sensor networks. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Nov. 7, Alexandria, pp: 89-96.

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

Eastlake, D. and P. Jones, 2001. US Secure Hash Algorithm 1(SHA1). RFC., United States, pp: 1-22.

Heinzelman, W.B., A.P. Chandrakasan and H. Balakrishnan, 2002. An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun., 1: 660-670.

Hou, T.C. and V. Li, 1986. Transmission range control in multi-hop packet radio networks. IEEE. Trans. Commun., 34: 38-44.

Kleinrock, L. and J. Silvester, 1978. Optimum transmission radii for packet radio networks or why six is a magic number. Proceedings of the IEEE Telecommunication National Conferance, December 1978, Piscataway, N.J., Institute of Electrical and Electronics Engineers, Inc., pp: 04.3.1-04.3.5.

Laurent, E. and V.D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, Nov. 18-22, ACM Press, Washington, DC. USA., pp: 41-47.

Li-Min, S. and F. Gui-Ming, 2005. A survey on energy efficient protocols for wireless. Commun. China Comput. Federation, 1: 1-10.

Liu, D. and P. Ning, 2003. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. Proceedings of the 10th Annual Network and Distributed System Security Symposium, Feb. 6-7, San Diego, CA., pp: 1-14.

Perrig, A., R. Szewczyk, J.D. Tygar, V. Wen and D.E. Culler, 2002. SPINS: Security protocols for sensor netowrks. Wireless Networks, 8: 521-534.

Rivest, R.L., 1994. The RC5 encryption algorithm. Proceedings of the 2nd International Workshop on Fast Software Encryption (FSE), Dec. 14-16, Leuven, Belgium, pp: 86-96.

Takagi, H. and L. Kleinrock, 1984. Optimal transmission ranges for randomly distributed packet radio terminals. IEEE. Trans. Commun., 32: 246-257.

Tany, H., S. Jha, D. Ostryz, J. Zic and V. Sivaraman, 2008. Secure multi-hop network programming with multiple one-way key chains. Proceedings of the 1ST ACM Conference on Wireless Network Security (WISEC), March 31-April 2, Alexandria, pp: 183-193.

Thai, T. and D.Z. Du, 2006. Connected dominating sets in disk graphs with bidirectional links. IEEE. Commun. Lett., 10: 138-140.

Xiao, X., X. Sun, X. Wang and L. Rao, 2009. DOSM: A data-oriented security model based on information hiding in WSNs. Inform. Technol. J., 8: 678-687.

Xu, Y., J. Heidemann and D. Estrin, 2001. Geography-informed energy conservation for ad hoc routing. Proceedings of the ACM International Conference on Mobile Computing and Networking, July 16-21, Rome, Italy, pp: 70-84.

Ye, F., H. Luo, S. Lu and L. Zhang, 2004. Statistical en-route filtering of injected false data in sensor networks. Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), March 7-11, Hongkong, China, pp: 2446-2457.