International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.105-116
http://dx.doi.org/10.14257/ijsia.2016.10.4.12

HSKAS: A Novel Hierarchical Shared Key Authentication Scheme in Wireless Sensor Networks

Zeyu Sun[12], Xiaohui Ji[1*], Yuanbo Li[1]

[1]*School of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang 471023, China.*
[2]*School of Electrical and information Engineering, Xi'an Jiaotong University Xi'an 710049, China*
jsjsdz@163.com

Abstract

Wireless sensor networks (WSNs) are often deployed in hostile environments, thus being subjected to great security risks. However, due to the influence of environment and dynamic topology, the communication radiuses of all nodes are no strictly consistent, which may cause different neighbor number and redundant neighbors for one central node. In this paper, we present a key agreement scheme without the trusted third parties by exploiting the special characteristics of Hopfield neural network: the two nodes converge in a steady state from their respective initial states after iterating finite times, while maintaining the confidentiality of the key by quantifying the key to strings. Compared to existing solution, the proposed method requires less memory and has lower communication overhead to key agreement.

Keywords*: wireless sensor networks; shared key; secure communications; Authentication Scheme*

1. Introduction

In wireless sensor networks (WSNs)[1-3], sensors are deployed in open environment of lacking infrastructure, the data is eavesdropped and even modified during transmissions and the measure to prevent eavesdropping is to construct a secure and authenticated link between two sensor nodes before communication, thus involving the key setup and distribution. So, how to achieve the shared key plays a very important role in establishing secure communications.

One challenge is that WSNs occurs unidirectional links. A sensor network consists of a collection of wireless nodes; each node can directly communicate with other nodes within its transmission range. The data is forwarded from source node to sink node by neighbor sensors using muti-hop routing scheme. Hence, numerous protocols are proposed to discover neighbor (cluster) sensors, such as ReIn-ForM [4],LEACH [5],GAF-[7],Top-Disc[8].all of them are assumed to be the same communication ranges. However, actually the wireless communication range is related to its power, the more powerful a sensor is, the larger communication range it has. On one hand, 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 number of neighbors are insufficient to maintain network connectivity

Xiaohui Ji is the corresponding author.

ISSN: 1738-9976 IJSIA

2. Related Work

Traditionally, general key agreement schemes can be classified into center and acentric control solutions based on whether key agreement depends on the trusted third parties (TTP). The center scheme depends on a trusted online key distribution center (KDC) [10]with adequate physical protection for a symmetry session key agreement, which is established by private keys which is shared with KDC between nodes. And the private keys in KDC need to be distributed using asymmetric cryptography, such as RSA schemes [7]. However, limited computation and power resources in sensor nodes often make public key algorithms infeasible. Moreover, due to communication range limitations among sensors and the lack of adequate physical shield, the KDC may be out of reach and the public key infrastructure (PKI)[9] for verifying public key is not available in WSNs. Independent of the above works, the key pre-distribution scheme[1,4,17] with offline TTP or on-line key setup servers was proposed, because the key information is distributed (stored in ROM) among all sensor nodes with few prior topology knowledge available before deployment, the key storage requirement at each node may be large. Moreover, rekeying (key update) is disabled post network deployment.

For the above-mentioned disadvantages, Diffie-Hellman [3] developed the acentric key agreement scheme based on the discrete logarithm problem (DLP), the session key is established dynamically in a peer-to-peer manner without the TTP, but a drawback discovered by [14] results in the man-in-middle attack when multiparty entities (malicious nodes) participate it. Recently, Suhas Mathur[2] has extracted a secret key from a wireless channel by exploiting special properties of the wireless channel, but the key establishment related to location is infeasible to node movement topology and too many redundant estimates incur high levels of communication overhead to reduce the bit-error probability .

Taking advantage of the peer-to-peer solution, we propose a key agreement scheme based on the special characteristics of Hopfield neural network: the two participating entities converge in a steady state from their respective initial states after iterating finite times, while maintaining the confidentiality of the key by quantifying the key to n-bit strings. That is, the probability that malicious nodes get the shared key is acceptably small. In our method, little memory is required for key stored, because the key is created dynamically and used until the current session is over, and then it is removed from the memory for the future session. Moreover, the node has lower communication overhead than the one proposed Suhas Mathur [2].There has been extensive research on wireless authentication protocol; Perrig *et al*. [12] proposeμTESLA, a security protocol for broadcast authentication. Liu and P. Ning [13] extend μTESLA to a two-level key ring structure. Based on above two level key rings scheme, Hailun[2] proposes a multi-hop authentication scheme with multiple one-way key chains, according to nodes hop distance to the base station. Deng, R. Han [3] proposes an authenticating scheme for defending against path-based DoS attacks; keys are picked from key chains when authenticating packet is sent each time. Another challenge is secure authentication. Due to sensors are deployed in open environment lacking infrastructure, nodes in the network without adequate protection may easily be captured, compromised, and hijacked by the adversary. As a result, 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, designing an authentication protocol suited for WSNs poses particular challenges. J. Deng, R. Han [3] proposes an authenticating scheme for defending against path-based DoS attacks. Keys are picked from key chains when authenticating packet is sent each time. If sending excessive packets, a large size of key chain is required to establish in advance and results in inadequate memory storage. Several schemes [2, 13] have been proposed to extend the μTESLA with multiple-level key chain to deal with the issue, but the scheme [2] 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.

3. Network Model

We introduce our novel technique, a secure Muti-hop authentication scheme, which consists of neighbor grouped discovery phase and packet verified phase. The core idea is hierarchical neighbors according to their communication range to the node and then Muti-hop authentication with keys derived from multiple low-overlap hash sub-chains. The network model is based on the following assumptions:

(1) Every node has the different transmission radius based on its power.
(2) The area of the network can be approximated as a square.
(3) Few nodes are mobile.

We combine our work with the principle of convergence in Hopfield neural network (HNN) [8] which is proposed by Hopfield. Different from forward neural network, it exist feedback state from output layer to input layer and it converges in a steady state where data is stored in finite time, which is titled as associative memory, thus being used to solve optimization problems. HNN is divided into discrete and continue model according to the activate mode. Discrete model means that only one cell changes its state using signal function every time. In this paper we only consider discrete model, which is composed of n cells which have interaction each other, the cell is fed back -1 state when it is suppressed, and is fed back +1 state when it is activated, therefore n cells may have $N=2n$ different states, the combination state set of n cells is denoted by the formula (1).

$$X_n = \left\{ \left(x_1 x_2 \cdots x_n \right) : x_i = -1 \text{or} 1, i = 1,2,3 \cdots n \right\} \tag{1}$$

The output of each cell i is fed back to all other nodes j (j=1, i−1, i+1, n) through weights w_{ij}. Assuming the weights are symmetric, the interaction from the j^{th} cell to the i^{th} cell is $W_{ij}x_j$, so the total output result from the whole HNN to the i^{th} cell is shown as formula(2)

$$Y_n = \sum_{j=1}^{N} W_{ij} x_j \left(t \right) \tag{2}$$

HNN runs automatically as follow: each cell is choose with the 1/n probability at t time, if the total output result of the i^{th} cell exceeds a threshold θ_i by inputting the cell state to a signal function that is given by formula (3) [8,15], the cell is active, denoted as +1; otherwise it is suppressed, denoted as -1.

$$x_j = sgn\left(\sum_{j=1}^{n} W_{ij} x_i - \theta_i \right) = \begin{cases} 1 & \text{active} \\ -1 & \text{suppressed} \end{cases} \tag{3}$$

So the state variation of every cell may lead a transformation from state set X_n to X_m according to formula (3). After iterating many times, HNN can converge in a steady state with minimum energy finally which is computed as formula (4)

$$E = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} W_{ij} x_i + \sum_{i=1} \sum_{j=1} \theta_i x_i \tag{4}$$

$$E\left(r \right) = k \left(2r \right)^n \tag{5}$$

$$T\left(e \right) = \frac{eR_{min}}{c} \tag{6}$$

$$e(R)=\left\lceil \frac{R}{R_{min}} \right\rceil \tag{7}$$

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 formula (7), and the transmission time $T(e)$ of packet p is defined by the formula(6).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[15-16].

The passed angle θ of query message for neighbor is derived by the formula (8). Where n denotes hop number that message is passed with the query angle α_i is specified randomly by query node, where i denotes query time, the incline angle β can be calculated as formula (9), and the process of neighbor discovery is illustrated in Figure1.

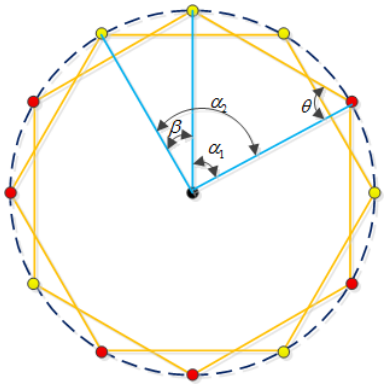

Figure 1. Nodes at an Angle of α_1 Degrees Sends a Query Message

By the formula (7), and the transmission time $T(e)$ of packet p is defined by the formula (6). 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.

$$\theta=\frac{\pi}{2}+\alpha+(2n-1)\beta \tag{8}$$

$$\sin\beta=\frac{1}{2e} \tag{9}$$

One nodes at an angle of α_1 degrees sends a token message, which appends a radio range R_i, a time stamp TAP of current nodes, transmission time $T(e)$, minimum radio range $R_{\min}$ and ID, When node A receives it, T=TAP_A-TAP_o 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 (5) is equal to $E(eR_{\min})$,if they are equal, the neighbor A is matched for nodes, it sends a feedback message with IDA to the nodes, subsequently, $T(e)$ and ID is updated by $T(1)$ and IDA, the query message is forwarded to next node B at an angle of θ_1 degrees. Otherwise, the same operation (only forwarding) as the matched case are performed with the exception, the feedback message being 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 message is sent by query node at angle of α_2 degrees increased, where α_i-$\alpha_{i-1}\leq 2k\beta$ (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.

4. Shared Key Using

We assume that only one cell transfers to next state through changing his weight every time, called serial model, and what is the next state of the cell is independent of its prior state in HNN. So the features possessed by the cell are coincident with Markov chain model [12], one cell's state is transformed from active to suppress or in reverse after importing the state to a signal function, while others' states keep original, so the probability of achieving the next state is 1/*n*, as shown in Figure (2). Therefore, when it is activated with enough times, it enters the reachable state finally, called associative state in HNNs. The matrix of transfer probability within one step is shown as the following formula.

$$P_{ij} = P\{X_j = p \mid X_i = q\} = \begin{cases} \sum_{1 \le n}^{n} \frac{1}{n} & p \neq q \\ 1 - P_{ij} & p = q \end{cases} \tag{10}$$

$$n = \lceil log_2 N \rceil \wedge s = p \oplus q \tag{11}$$

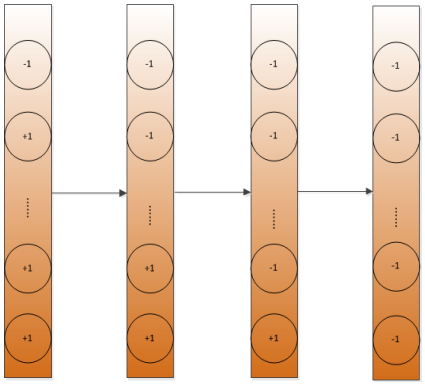

Figure 2. The State Transfer of *n* Cells

In WSN environment, the number *N* of states is related to the network size. That is to assure that every node is likely to get a different state from *X*n. the shared key establishment is initiated by a transmitter (A as the transmitter) who wants to communicate confidentially with a receiver (B as the receiver). First of all, A generates target state T and key size *i*, which is transmitted to B. Then A and B create randomly an initial state XA and XB respectively from state space using formula (1), A and B adjust weights automatically using the formula (1), A and B adjust weights automatically using δ learning rule [13], so that they can converge in a minimum energy, which serves as a bit shared key using the quantize $Q(E)$ as follow , where t is a certain threshold based random-ness criteria for key bit. Then WA and WB are updated for the next bit key agreement. After iterating *i* times, the *i*-bit key is established between A and B. The detailed steps are shown in below algorithm and Figure (3).

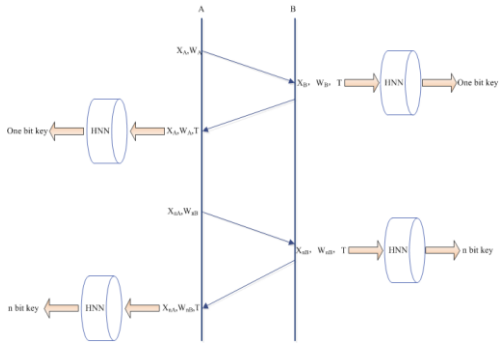

Figure 3. Timing Diagram for the Key Agreement Algorithm

We take the HNNs with four cells (N=16) as an example to illuminate how one bit shared key is achieved. So each cell exists in possible sixteen different states, the combination state space of four cells is shown as the following formula:

$$X = \{X_0 = -1-1-1-1, X_1 = 1-1-1-1, \cdots, X_{15} = 1111\} \tag{12}$$

The threshold t to guarantee key bit randomness is -10 and the threshold θ_n for HNN is shown as the following formula:

$$\theta = \{\theta_1, \theta_2, \theta_3, \theta_4\} = \left(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) \tag{13}$$

A and B create randomly an initial state XA and XB respectively from X, symmetrical matrix of weights WA and WB , for example Alice chooses X8 and Bob selects X14, WB is shown as the following formula, where l /n denotes the proportion of weight.

$$W_B = \frac{l}{n}\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix} \tag{14}$$

A sends a target state T to Bob. After receiving it, B begins to transfer X14 as follow: shown as Figure (3), while the fourth cell in B is selected, it is changed from active to suppress after importing the state to a signal function, but other three states keep original. So B achieves the state X6 from X14, the combination state transfer probability within one step is 1/4.

We propose a distributed hierarchical scheme employing multiple one-way hash [11] sub-chains instead of the entire chains which Hailun Tany [2] adopted to secure authentication. A hash chain consists of multiple sequence values K_0, K_1, K_2, …, K_n, Subsequent values K_i , for i: $n>i\geq 0$, 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 i^{th} sequence values from e^{th} layer hash chain is denoted as K_i^e . In initialization, correspondence layer neighbors are deployed initially with K_0^1 , K_0^2 , K_0^3 … K_0^e 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 i^{th} 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[12]), which is denoted as the $ring_i = \{ C_k^1, C_k^2, C_k^3, \ldots C_k^e \}$,the element C_k^e in set indicates that *k* hash keys elements are selected randomly from e^{th} layer 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 $\{ K_0^1, K_0^2, K_0^3 \ldots K_0^e \}$ with discussed above scheme.

Algorithm: Key agreement between A and B

Input: key size *i* and network size *N*

Output: *i* bits key

A: X_A generated

B: X_B generated

A→B:*i*

While ($i \neq 0$)

{

{ A: W_A generated

B: *T* and W_B generated

A & B : converge at *T* in HNN

A & B : co**mpute energy *E* of *T* }**

if ($E>T$) then

$Q(E) \leftarrow 1$

else

$Q(E) \leftarrow \mathbf{0}$

i++

}

When source node A sending a packet, it picks a K_i^x randomly from i^{th} sub-chain C_i^x 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_i^x to B, as B receives it. Assuming B has a previous key K_j^x in its key pool, if *i* is not greater than j, B obtains the hash element $(K_i^x)'$ by performing (j-i) times hash computation for K_i^x until j is reduced to *i*. B then informs A that the packet appending the MAC which is computed with $H(M \| K_i^x)$ can be sent .after receiving it , B then may verify whether $H(M \| (K_i^x)')$ is identical with MAC or not ,equality between them indicates that the M is not modified by the malicious node during transmission. At the same time, the previous stored key K_j^x in memory is replaced by the $(K_i^x)'$. Otherwise, the packet 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 $(K_j^x)'$ by performing (*i-j*) times hash computations for K_j^x until i is reduced to *j*,

subsequently, A sends the packet appending the MAC which is computed with $H\left(M\|\left(K_j^x\right)'\right)$ to B, after receiving it, B verify whether $H\left(M\|K_j^x\right)$ is equal to MAC or not, if both are the same, the packet is authorized and K_i^x in A is replaced by. Otherwise, it is discarded. The detailed steps are shown in below Algorithm.

Algorithm: Verification Between node A and B

Input: Packet M

Output: Whether Mis authorized or not

A selects a K_i^x from i^{th} sub-chain C_i^x in the ring according to layer key choosing scheme

A→B:*i*

B: receive *i*

if (*i*≤*j*) then

B: $\left(K_i^x\right)' \leftarrow H\left(\cdots H\left(K_j^x\right)'\right)$

A→B: $M\|H\left(M\|\left(K_i^x\right)'\right)$

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

B:accept M

else

B:drop M

end if

else if (*i*>*j*) then

B→A:*j*

A:receive *j*

A: $\left(K_j^x\right)' \leftarrow H\left(\cdots H\left(K_i^x\right)'\right)$

A→B: $M\|H\left(M\|\left(K_j^x\right)'\right)$

if ($H\left(M\|\left(K_j^x\right)'\right) == H\left(M\|K_j^x\right)'$)then

B: accept M

else

B:drop M

end if

end if

5. Performance Evaluation

In our scheme, the shared key is created dynamically in the local when communication and used until the current session finishes. One node needs stores weight matrix, initial state, target state, shared key size i and algorithm S_a (expressed in bytes) including key agree-ment and symmetrical matrix storing. The memory space W (expressed in bits) can be shown in the formula below:

$$W = \left(\lceil log_2 N \rceil^2 + 10\lceil log_2 N \rceil\right)/2 + i + 10S_a \tag{15}$$

We compare the memory space taken (algorithms for symmetrical matrix storage and key agreement take 20bytes) per node to get 32 bits shared key of our scheme with that of R-KPS.

The Figure 4 shows that the network size N has little obvious impact on the memory space taken per node to establish keys in our scheme, but has a direct impact on the memory required in R-KPS—increasing the node number requires more memory space per node and decreasing the node number has the opposite effect. Moreover, the node of our scheme has less memory space than that of the R-KPS scheme, because the key is created dynamically and used until the current session is over, and then it is removed from the memory for the future session.

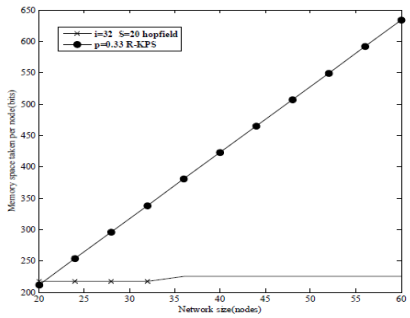

Figure 4. The Memory Comparison with R-KPS and Proposed Scheme per Node to Get 32 Bits Key

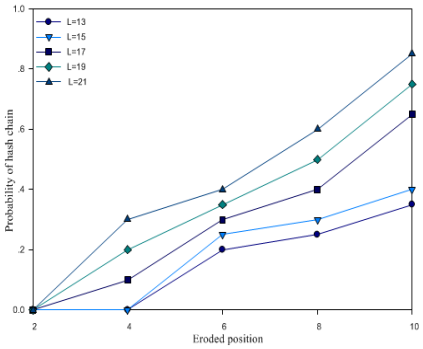

Figure 5. The Probability Comparison of Occurring at all Layers

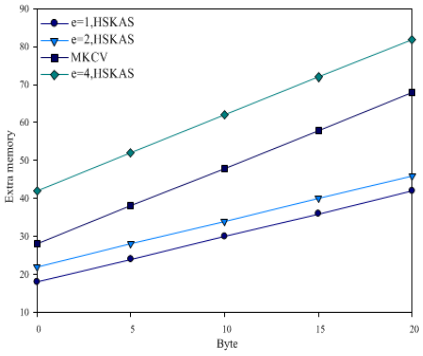

Figure 6. Extra Memory Comparison of Forward Node with the HSKAS

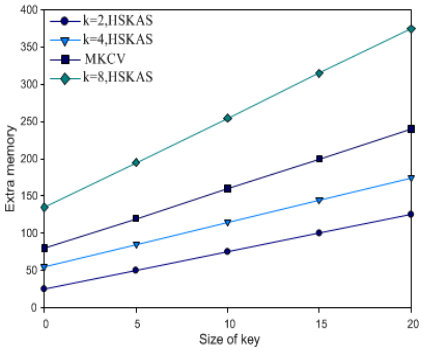

Figure 7. Extra Memory Comparison with HSKAS in Sensing Source Node

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 13,15,17,19and 21, respectively), under the assumptions given α=0.1. It is believed that the security improvement in increase of chain length L outweighs the decrease of the eroded position d. 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 Figure 5.

The comparison of extra memory space in each node (except for sensing nodes) results, using the HSKAS scheme and multiple one-way key chains verification (MKCV) scheme, are shown in Figure 6 and Figure 7. The results show that the HSKAS scheme proposed has smaller extra memory space than original MKCV scheme, when e=2 and c is smaller than 18bytes, the similar results are as shown in the case of e=3, c<9bytes and the case of e=4, c<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 a initial key randomly from key pool to verify packets. Consequently, the extra memory space in sensing source node in our scheme can be defined in formula:

$$W_{sense} = (c+8) * e * k \tag{16}$$

We compare the extra memory space taken of sensing nodes in our scheme with the base station in MKCV scheme. The results show in Figure7 that the sensing source node has smaller 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.

6. Conclusion

In this paper, we have introduced a key agreement scheme for secure communication between two participating entities. The essential idea is to combine key agreement with

the principle of convergence in Hopfield neural network, while resisting the brute force attacks for the key by quantifying the key to i-bit strings. 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 redistributions phase to reduce the energy consumption and communication overhead, we further validated the eroded probability in Hash chains to alleviate jeopardy from internal attack launched by an adversary. We have also shown experiment results that our technique requires less memory and has lower com-munition overhead than the existing scheme.

Acknowledgments

Projects (61170245,U1304603) supported by the National Natural Science Foundation of China; Project (2014B520099) supported by Henan Province Education Department Natural Science Foundation; Project (142102210471,142102210063, 142102210568) supported by Natural Science and Technology Research of Foundation Project of Henan Province Department of Science; Projects (1401037A) supported by Natural Science and Technology Research of Foundation Project of Luoyang Department ; Projects (2014M561324) supported by Postdoctoral Science Foundation of China; the science and technology research project of education department of Henan Province (14A510009), the funding scheme for youth teacher of Henan Province (2012GGJS-191);

References

[1] G Ang , W Wei, W Zhixiao, W Yan. "A Hierarchical Authentication Scheme for the Different Radio Ranges Sensor Network". 2009 International conference on Computational Science and Engineering, Miami, USA, **(2009)** Sept 494-501.
[2] T Hailun, J Sanjay. O Diet, Z John, "Vijay S. Secure multi-hop Network Programming with Multiple One-way Key Chains". Proceeding of the first ACM Conference on Wireless Network Security, Kyoto, Japan, **(2008)** Feb 206-211.
[3] G Ang, W WeI, W Zhi. "Hopfield-Association: Establishing a shared Key in the Wireless Sensor Networks. 2010 Second International Conference on Networks Security", Wireless Communications and Trusted Computing, ShangHai, China **(2010)** Jun 70-73.
[4] J Deng, R Han, S Mishra, "Defending Against Path-based Dos Attacks in Wireless Sensor Networks". Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, London, UK, **(2005)** Apr, pp. 195-199.
[5] Z Zaohong . "Analysis of Influencing Factors of Blackboard Teching Effect Based on Ism Model". IIETA International Information and Engineering Tchnology Association, vol.1, no.2, **(2014)**, pp.9-12.
[6] X Luxin, "Research on The Optimization of Enrollment Data Resources Based on Cloud Computing Platform". IIETA International Information and Engineering Tchnology Association, vol.2, no.2 ,**(2015)**, pp.1-6.
[7] H Chan, A Perrig, D Song. "Random Key Predistribution Schemes for Sensor Networks". IEEE Symposium on Security and Orivacy,vol.27, no.2,**(2003)**, pp.56-67.
[8] M Suhas, T Wade, M Narayan, Y Chunxuna, R Alex, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel", Proc of ACM MobiCom, Atlanta,USA,**(2008)**, Feb, pp. 236-242.
[9] D Whit, H Martin, "New directions in Cryptography". IEEE Transactions on Information Theory, vol.21, no.12, **(2010)**, pp.962-977.
[10] L Eschenauer, V D Gligor, "A key-Management Scheme for Distributed Sensor Networks". Proc of ACM CCS02, Augusta, USA,**(2002)**, Jan, pp. 520-523.
[11] F Ye, H Luo , S Lu, L Zhang. "Statistical Route-filtering of injected false data in Sensor Networks Proceeding IEEE INFOCOM", Denver, USA**, (2004)** May, pp. 453-457.
[12] Y Xu, Heidemann, J Estrin. Geography-informed energy conservation for Ad Hoc Routing. Proc 7th Annual intel Conf on Mobile Computing and Networking, Kobe, Japan, **(2001)** May, pp. 56-59.
[13] S Liming, G Guiming, "A Survey on Energy Efficient Protocols for Wireless. Communications of China computer Federation (CCF)", Dalian,China, **(2002)** Oct, pp. 13-16.
[14] F Xue, P R Kumar, "The Number of Neighbors Needed for Connectivity of Wireless Networks". Wireless Networks, vol.26, no.9, **(2002)**, pp.1254-1263.
[15] A Perrig, V Szewczyk, D C Wen, J D Tygar. "SPINS: Security Protocols for Sensor Networks. Journal of Wireless Networks",vol.17,no.10, **(2002)**, pp.521-534.

[16] G G Savo. "Optimal Transmission Radius in Sensor Networks. Advanced Wireless Sensor Network: 4G Technologies", John Wiley & Sons Ltd, vol.19, no.2, **(2006)**, pp.568-571.

Authors

Zeyu Sun, was born in 1977 in Changchun city, jilin province, in 2010 graduated from Lanzhou university, Master of Science; xi 'an Jiao tong university study for PhD at present. He is a lecturer in Luoyang institute of technology of computer and information engineering, is also a member of China computer society. The main research interest is in wireless sensor networks, parallel computing and Internet of things.

Xiaohui Ji (1978-), born in Luoyang City, Henan Province, a lecturer of Luoyang Institute of Science and Technology Computer and Information Engineering Department. Her main research interests include artificial intelligence and parallel.

