J. Basic. Appl. Sci. Res., 2(10)9918-9924, 2012

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Identifying the Insecure Paths as a Means of Pair-Wise Path Key in the Wireless Sensor Network

Mohammad Amin Sadeghi Joola[a], Adel Sarmast[b], Amir Masoud Bidgoli[c], Mohammad Behrouzian Nejad[d]

[a,d]Young Researchers Club, Dezfoul Branch, Islamic Azad University, Dezfoul, Iran
[b]Department of Computer, Dezfoul Branch, Islamic Azad University, Dezfoul, Iran
[c]Department of Computer, North Tehran Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

The provision of security measures for the wireless sensors in military or similar applications is of vital importance. The use of coding keys for enhancing the secrecy of data and ascertaining their originality is considerably increasing and various methods have been introduced to position these keys in the nodes. The method involved common keys already mounted in the memory system and pre-distributed. Under circumstances where no common key is among the nodes, the nodes between the sensors are used. Given that these nodes might be prawn to compromise, there is a chance that the data might be exposed to unauthorized uses. Various methods for positioning the keys between the nodes have been proposed which are able to detect the malicious node in this route but none of which has been able to detect various malicious nodes. The paper aims to identify the insecure paths with various malicious nodes. Results showed that the proposed algorithm has lower energy consumption and by increasing the number of routes the proposed algorithm will have a better efficiency.
KEYWORDS: insecure routs, Wireless Sensor Network (WSN), key management

I INTRODUCTION

WSN includes sensor nodes with low power and broadband and low processing power in insecure environment which are distributed to obtain data from environment [1, 2] .These characteristics enable the system to establish security measures in order to prevent access to unauthorized data from the network. One of the security components is the establishment of the key in the system.

Given the specific features of the WSN and the use of tiny batteries in the sensor nods to supply the required energy, it would not be possible to use the keys in the system [11, 12]. Various pre-distribution key techniques have been introduced in the literature [13-22]. For instance, in [13] the base station incorporates a set of keys in each node memory which randomly pre-distribute M keys [4,6-8,16]. Pair-wise path key establishment have been introduced which enhance the security in communication and in case of compromise by one or more nodes, the data from other paths would not be exposed to unauthorized users. The problem arises where two nodes in the network that do not have a common key need to have key establishment via their intervening paths [15]. This is particularly exacerbated where intervening nodes in the path are compromised and as such the data are exposed to unauthorized users. For this reason the use of pair wise keys from various paths will enhance the operational security of the network despite having some limitations. One such challenge is the possibility of communicating inaccurate data due to compromised nodes in the network. In [3] a method has been introduced to detect the compromised nodes according to which the key K is equally divided by M parts, each of which reaches the destination from disjoined paths. According to this technique the compromised nodes can be identified through a hop-by-hop mechanism. However, this method would not be able to detect the insecure paths because the compromised nodes can easily bypass the security measures.

The aim of this paper is to provide a methodology for solving the above problem. As in this paper we proposed a methodology to solving the above problem by use of an analytical model and show the potential of the method in detecting the unsecure routes. Unlike the method [3], proposed method can detect the insecure paths.

The remainder of the paper was organized as follows: In section II, we gives related works in section III, we describe our proposed scheme in details. Then the performance evaluation with analysis result describe in section IV. Finally, section V concludes this paper.

II related work

J.P.Sheu and et all [3] survey Pair-wise path keys problem. In this approach the base station set keys in memory nodes before pre-distributed. After create network, all network environment divide to several cells And any

***Corresponding Author:** Mohammad Amin Sadeghi Joola, Young Researchers Club, Dezfoul Branch, Islamic Azad University, Dezfoul, Iran

node specific your id and your group id and then sends those to your one-hop neighbors and searches shared key between itself and one-hope neighbors.

If doesn't shared key between two nodes, then this nodes establish shared key between own by shared neighbors.

If number of paths between these nodes are $n \geq 3$, the start node divide key to N segment and send to destination node any segment by one of N paths.

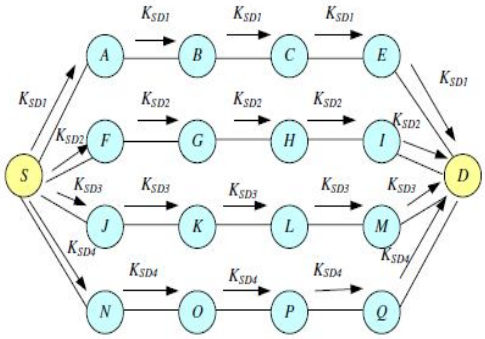


Figure (1): An example of multi-path key establishment with the (3, 4) secret sharing scheme.

In this state assuming source node and destination node are not captured by enemy. If node S wants to establish a key with node D, node S must generate a hash key chain before finding the node-disjoint paths. Therefore, S chooses a random value x and computes the list of values h0, h1, h2, . . . ,hm, where $h_0 = x$ and $h_{(i)} = H\left(h_{(i-1)}\right)$, for 0 < i 5 m. The intermediate nodes use of this key for authentication nodes that are itself before. Furthermore assume that the destination and intermediate nodes establish shared key with one and two nodes before itself.

After finding the n disjoint paths, the source node(S) divides the path key $K_{(SD)} = SK_{(1)} USK_{(2)} U..USK_{(n)}$ Node S sends each key segment SKi, $1 \leq SK_{(i)} \leq n$ through the i-th secure node-disjoint path. Stages of algorithm key-path establishment are following [3]:

Assume that S and D nodes want establishing shared key-path.

For S node:

Step1: The source node divide $K_{(SD)}$ key to N segment. $\mathrm{SK}_{(\mathrm{i})} \quad \text{for} \quad 1 \leq \mathrm{i} \leq \mathrm{n}$

Step2: Assuming the i-th node-disjoint path consists of Nodes $S_{(i)}, a_{(1)}, a_{(2)}, ...a_{(m)}, D$. The source node encrypts the i-th key segment $SK_{(i)}$ with the pair-wise keys of its one-hop and two-hop neighbors denoted as and $K_{(S,a_1)}\{SK_{(i)}\}, K_{(S,a_2)}\{SK_{(i)}\}$.

Step3: On the i-th node-disjoint path, the source node will send the $K_{(S,a_1)}\{SK_{(i)}, MAC_{(h(m-1))}\{SK_i\}\}$ and $K_{(S,a2)}\{SK_{(i)}, MAC_{(h(m-1))}\{SK_i\}\}$ messages to its next one-hop and two-hop neighbors. To achieve two-party authenticity and data integrity, we use a message authentication code (MAC). The following notations are used to denote the messages send from the source to its next one-hop and two-hop neighbors, respectively.

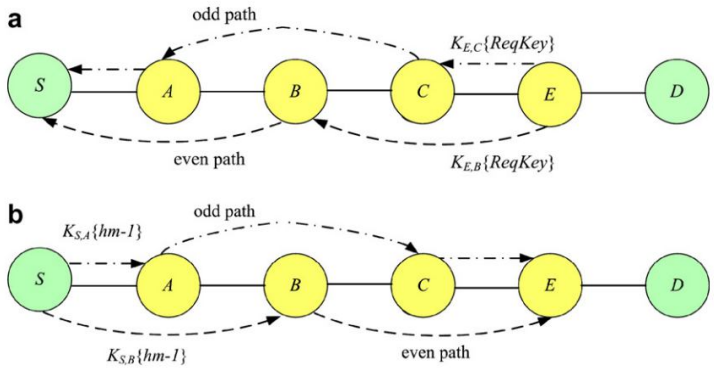
$$S \rightarrow a_{(1)} : K_{(s,a1)}\{SK_{(i)}, MAC_{(h(m-1))}\{SK_{(i)}\}\} \quad (1)$$

$$MAC_{(K(S,a1))}\{K_{(S,a1)}\{SK_{(i)}, MAC_{(h(m-1))}\{SK_{(i)}\}\} \quad (2)$$

$$S \rightarrow a2 : K_{(s,a2)}\{SK_{(i)}, MAC_{(h(m-1))}\{SK_{(i)}\}\} \quad (3)$$

$$MAC_{(K(S,a2))}\{K_{(S,a2)}\{SK_{(i)}, MAC_{(h(m-1))}\{SK_{(i)}\}\} \quad (4)$$

Step 4: If source node receives ReqKey from the odd and even paths(showed in Fig(2) a,b), it encrypts the undisclosed hash key $h_{(m-1)}$ with its next one-hop and next two-hop pair-wise key and forwards the encrypted message to the requested node through the reverse odd and even paths.



Fig(2): An example of key disclosure procedure through the odd path (the dot dash line) and the even path (the dash line) forwarding.

For each intermediate node $aj \quad 1 \le j \le m$:

Step 1: If the received messages from its preceding one-hop and two-hop neighbors are consistent, it forwards the received messages to its next one-hop and two-hop neighbors.

Step 2: If the received data from its preceding one-hop and two-hop neighbors are inconsistent, the intermediate node a_j encrypts a ReqKey message with its preceding one-hop and two-hop neighbors' pair-wise keys, and sends the encrypted ReqKey to the source node via the odd path and even path.

Step 3: When the intermediate node receives the disclosed hash key $h_{(m-1)}$ it verifies whether the key is sent from the source node by checking $H\left(h_{(m-1)}\right) = h_{(m)}$ if the key is verified as sent from the source node, the intermediate node can identify who is a malicious node by computing the MAC of key segment with the hash key $h_{(m-1)}$. Destination node D has same procedure.

Proposed algorithm in [3] however can detecting malicious nodes but can't detect those if two or more malicious nodes are neighbor in one path.

III Proposed algorithm and assumptions

A the network model and assumptions

The assumptions of the paper are based on the proposition that the sensor nodes are related to the central station in the form of the multi-hops and the nodes are fixed. It is the central station which is resistant to compromise. There is a possibility for the nodes in the network to come under attack, and only the source and destination nodes are resistant to and therefore protected against the attack.

B Proposed Algorithm

The proposed algorithm is of a multi-path form by which to identify the insecure paths in the time of establishing pair wise path key. The existence of two or more malicious nodes in its vicinity along the route renders the path as insecure or under the condition of two nodes making it possible to send false data the algorithm in 3 will be unable to identify the insecure paths. For this reason, after completing the algorithm process the key establishment which has been incorporated in [3], our proposed algorithm operates as follows:

For any intermediate nodes $a_{(j)}\left(1 \le j \le m\right)$:

Step1: Under circumstance that the intermediary node a_j identifies the malicious node prior to it by $h_{(m-1)}$ key sending the source node, the message is send to the one prior to the malicious node. If the latter is of one-hop that is prior to the one in question, the malicious node ID is sent to the node two-hop prior to it. Under circumstances that the malicious node is two-hop prior to it, the sending of malicious node's ID is done in two phases in such a form that it send the malicious ID to a node prior to it, and the latter in turn sends it to two nodes prior to it

The following semi-code shows the sending processes of the malicious node:

If Malicious node = a_{j-1} {
$a_j \rightarrow a_{j-2}$: K(a_j , a_{j-2} {ID (a_{j-1})},
MAC $_{(a_j, a_{j-2})}$ {ID (a_{j-1})}

If Malicious node = a_{j-2}
$\{a_j \rightarrow a_{j-1}$: K($a_j$, a_{j-1}) {ID (a_{j-2})},
MAC (a_j ,a_{j-1}) {ID (a_{j-2})}
$a_{j-1} \rightarrow a_{j-3}$: K ($a_{j-1}$,$a_{j-3}$) {ID ($a_{j-2}$)},
MAC (a_{j-1},a_{j-3}) {ID (a_{j-2})}

The ID in the semi-code provided shows the malicious node.

Step2: When the destination node (D) receives the last part of the node from the route j, $1 \leq j \leq m$, an authentication message is send to the original point from the same route in order to inform the sending point.

Step3: After receiving the ack message by the sender, given, , n separate route , the n will produce MAC message , the structure of each MAC message will have the following form $MAC_{(i)}\{h_{(j)}, SK_{(i)}\}$:
Where i=j
For example based on figure 1, the s node will produce the keys in eq.5:

$$h_{(1)}, h_{(2)}, \ldots h_{(m)} \quad 1 \leq j \leq M$$

$$\begin{array}{l} MAC_1 \{h_{(1)} , SK_{(1)}\} \\ MAC_2 \{h_{(2)} , SK_{(2)}\} \\ MAC_3 \{h_{(3)} , SK_{(3)}\} \\ MAC_4 \{h_{(4)} , SK_{(4)}\} \end{array} \qquad (5)$$

Step4: After that, provide that the message number MAC is not similar to the route number, the generated messages MAC are sent from each route. In other words having n separate routes n-1 MAC message should be sent from each route. After sending the MAC messages from the sender node, each intermediate node which identifies the undesirable node after it will encode the received message and subsequently send to its two-staged node, where it is decoded.

Step5: After receiving the MAC messages from every route by the destination node, it could identify the insecure routes by comparing them.

For example, under circumstances where three separate routes exists between sending and receiving nodes and givens that the route 1 is insecure, and the $SK_{(1)}$ key in this route, is not genuine, under conditions where it receive $MAC(SK_{(1)})$ from 2 and 3 paths, route and given that the two MAC obtained from the routes 2 and 3 they would be compared with those messages from route 1. The proposed algorithm will be able to detect K insecure route, given n route separate by eq.6.

$$\begin{cases} \text{If N mod 2=0 then } K = \left(\frac{n}{2}\right) - 1 \\ \text{If N mod 2}\neq 0 \text{ then } K = \left(\frac{n}{2}\right) \end{cases} \qquad (6)$$

IV VALUATION OF ACT AND ANALYSIS RESULTS

A overhead memory

In order to evaluate the performance algorithm two overhead communication and memory criteria are taken into consideration. Given the n routes between two nodes, the destination node has to receive and store $n \times (n-1)$ MAC messages from the base node to identify the insecure route. This is needed to compare the MAC messages. For example, with 5 routes the destination node receives 20 MAC and subsequently after identifying insecure routes, the messages are deleted from memory. Therefore the overhead memory is negligible and by using the 4 bite keys, 80 bites are occupied from the memory for a short period which has a negligible overhead memory.

B Communication overhead

Under circumstance that N disjoint path between source node and destination nodes, for detection unsecure paths can using of following method. Source node can send 4 MAC massage in one packet.

Number of packets that the source node can send equal with eq.7.

$$\begin{cases} n & 3 \le n \le 5 \\ 2n & 6 \le n \le 9 \\ 3n & 10 \le n \le 13 \end{cases} \quad (7)$$

In other where under circumstance existence X intermediate malicious nodes in disjoint paths that detected in before stage, and under circumstance existence Y send packets from source node for detect unsecure path, communication overhead is 4XY in intermediate nodes. One very serious point in proposed algorithm is decreasing communication overhead than proposed algorithm in [3]. For example, proposed algorithm in [3] for a path with 5 intermediate nodes and without malicious nodes, number 10 messages shod be sending but proposed algorithm in this paper only need to sending 5 massages therefore has less consume energy. Furthermore in intermediate nodes can't processing tasks and encryption over packets that are received. But in [3], the intermediate nodes must achieve processing task and re-encryption over any pockets. Whenever told relatives about communication overhead and if assume that energy consume for send a byte equal to 2.95 μj and receive equal to 6.28 μj [9] then can get energy consume for detect unsecure paths.

Parameter	Amount	Description
N	100	Number of nodes in network
S	10	Number of source nodes
D	10	Number of destination nodes

Table (1): Assumption

In this model assume that exist a network with 100 nodes (N) and existing 10 source nodes (S) and 10 destination nodes (D) in pair-wise path key establishment. Figure (2) show energy consume for communications in proposed algorithm with 10 nodes, aim sending data and figure(3) show energy consume for communications in proposed algorithm with 10 nodes, aim receiving data.
Figure (4) show energy consume of intermediate nodes for sending packets. Under circumstance figure (4), we understand that energy consume for communication is very low and communication overhead is very little in our proposed algorithm.

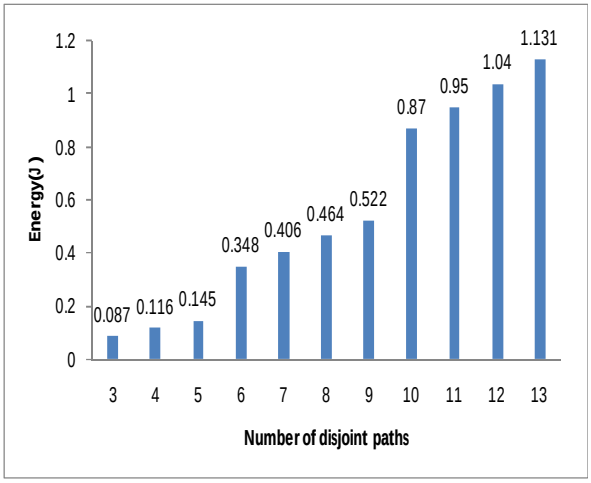


Figure (2): energy consume for communications in proposed algorithm with 10 nodes, aim sending data.

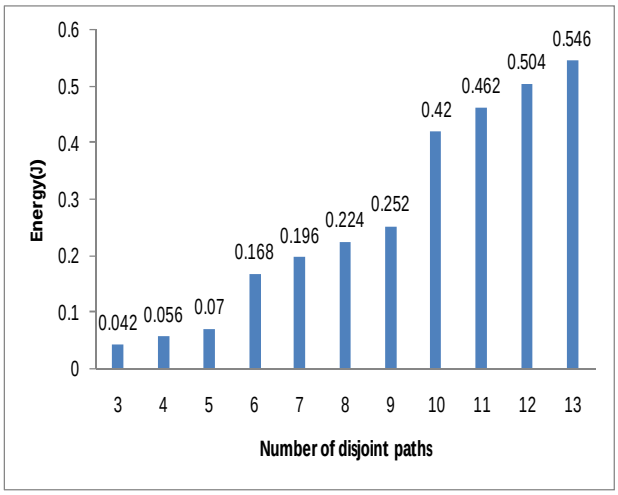


Figure (3): energy consume for communications in proposed algorithm with 10 nodes, aim receiving data.

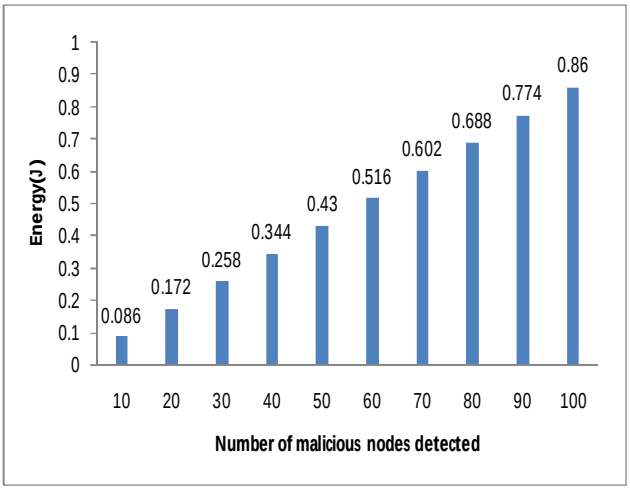


Figure (4): energy consume in intermediate nodes, aim communications in our proposed algorithm.

V Conclusion

Many methods for positioning the keys between the nodes have been proposed which are able to detect the malicious node in this path but none of which has been able to detect two or more malicious neighbor nodes in one path (unsecure path). In this paper, we consider unsecure paths detection problem in pair-wise path key establishment and propos a method for detection these paths. Then valuation this method with present two scales. Results show that my proposed algorithm has little communication and memory overhead and probability detecting unsecure path is increased if increasing the number of paths between two nodes.

VI REFERENCES

[1]I.F.Akyildiz, W.Su,Y. Sankarasubramaniam, and E.Cayirci, "Wireless Sensor Networks: a Survey Computer Networks", Vol. 38,No. 4,pp. 393–422,March 2005.

[2]I.F.Akyildiz, W.Su, Y.Sankarasubramaniam and E. Cayircl, **"**a Survey on Sensor Network**"**, IEEE Communication Magazine, Vol. 40,pp. 102-114,August 2002.

[3] J.P.Sheu , J.C. Cheng, "Pair-wise Path Key Establishment in Wireless Sensor Networks", Computer Communications, Vol.30, No.11-12, pp.2365-2374, September 2007.

[4] H. Chan, A. Perrig and D. Song, "Random Key Pre-distribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy, pp. 197–213, May 2003.

[5] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks, MobiCom '00, pp. 56–67 Aug 2000.

[6] S. Zhu, S. Xu, S. Setia, S. Jajodia, "Establishing Pair-wise Keys for Secure Communication in Adhoc Networks: a Probabilistic Approach in" 11th IEEE International Conference on Network Protocols, November 2003.

[7] H. Ling, T. Znati," End to End Pair-wise Key Establishment using Multi-path in Wireless Sensor Network",IEEE Global Communications Conference, December 2005.

[8] G. Li, H. Ling, T. Znati, ''Path Key Establishment using Multiple Secured Paths in Wireless Sensor Networks", ACM Conference on Emerging Network Experiment and Technology , pp. 43–49, 2005.

[9] A.S. Wander, et al.," Energy Analysis of Public-key Cryptography for Wireless Sensor networks", PerCom '05, Third IEEE International Conference on Pervasive Computing and Communication, March 2005.

[10] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures", IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA'03), pp.113–127, 2003.

[11] A.D. Wood, J.A. Stankovic, "Denial of Service in Sensor Networks", IEEE Comput. Vol.3, pp.54–62, 2002.

[12] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks", INFOCOM'04, pp. 2446–2457, March 2004.

[13] L. Eschenauer, V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", the 9th ACM Conference on Computer and Communication Security, pp. 41–47, November 2002.

[14] D. Huang, D. Medhi," A Byzantine Resilient Multi-path Key Establishment Scheme and its Robustness Analysis for Sensor Networks", the 19th IEEE International Parallel and Distributed Processing Symposium, 2005.

[15] W. Du, J. Deng, Y.S. Han and P.K. Varshney, "A Pair-wise Key Predistribution sScheme for Wireless Sensor Networks", the 10th ACM Conference on Computer and Communication Security, pp. 42–51, October 2003.

[16] D. Liu, P. Ning," Establishing Pair-wise Key Establishments in Distributed Sensor Networks",10th ACM Conference on Computer and Communications Security, pp.52–61, October 2003.

[17] W. Du, J. Deng, Y.S. Han, S. Chen and P.K. Varshney, "a Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge",IEEE INFOCOM, March 2004.

[18] D. Liu, P. Ning, Location based Pair-wise Key Establishments for Static Sensor Networks, the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks , pp. 72–82, 2003.

[19] D. Huang, M. Mehta, D. Medhi and H. Lein," Location aware Key Management Scheme for Wireless Sensor Networks",ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 29–42,October 2004.

[20] Y. Zhou, Y. Zhang, Y. Fang, "LLK: a Link Layer Key Establishment Scheme in Wireless Sensor Networks", IEEE Wireless Communications and Networking Conference, pp.29–42, March 2005.

[21] Z. Yu, Y. Guan, "a Robust Group-based Key Management Scheme for Wireless Sensor networks", IEEE Wireless Communications and Networking Conference, 2005.

[22] H. Chan, A. Perrig, "PIKE: Peer Intermediaties for Key Establishment in Sensor Network", IEEE INFOCOM, March 2005.

[23] M.Y. Hsieh, Y.M. Huang, "a Secure On-demand Source Routing with Distributed Authentication for Trust-based Adhoc Networks", LNCS 3779, pp. 343–350, 2005.