Alghamdi *Hum. Cent. Comput. Inf. Sci.* (2019) 9:38
https://doi.org/10.1186/s13673-019-0198-1

Human-centric Computing and Information Sciences

RESEARCH Open Access

Convolutional technique for enhancing security in wireless sensor networks against malicious nodes

Turki Ali Alghamdi*

*Correspondence:
taghamdi@uqu.edu.sa
Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia

Abstract

Wireless sensor networks (WSNs) comprise tiny devices known as sensors. These devices are frequently employed in short-range communications and can perform various operations such as monitoring, collecting, analyzing, and processing data. WSNs do not require any infrastructure, are reliable, and can withstand adverse conditions. Sensor networks are autonomous structures in which the sensor nodes can enter or leave the network at any time instant. If the entering node is attacker node it will monitor the network operation and can cause security issues in the network that can affect communication. Existing literature presents security improvements in such networks in the form of cryptography, asymmetric techniques, key distribution, and various protocols. However, these techniques may not be effective in the case of autonomous structures and can increase computational complexity. In this paper, a convolutional technique (CT) is proposed that generates security bits using convolutional codes to prevent malicious node attacks on WSNs. Different security codes are generated at different hops and the simulation results demonstrate that the proposed technique enhances network security and reduces computational complexity compared to existing approaches.

Keywords: Convolutional technique, Sensor, Security, Wireless sensor networks

Introduction

Wireless sensor networks (WSNs) are used for wireless data transfer from source to destination by employing sensors as intermediate nodes. Sensors are capable of storing and processing limited volumes of data. WSNs were primarily developed for complex military communications that do not support wired networks. The wireless sensors are spatially distributed, self-organized, and can form a network without any predominant structures. Sensors are mobile and can enter or leave the network at any time instant. This nature of sensor mobility creates security concerns related to malicious node attacks on of the network. The authors in [1, 2] present a discussion on the importance of security at different levels of network communication. The authors also presented different techniques for securing sensor networks, including network requirements.

In terms of securing such networks, a method commonly discussed in the existing literature is cryptography, which involves securing the original data through a key. The

same key may be used for data encryption and decryption (symmetric cryptography) or there may be a different key for encryption and another for decryption (asymmetric cryptography). The keys used in cryptography consume significant energy and storage space, which are limited resources in WSNs. In addition, key distribution is complex because it is distributed to all nodes in the network, irrespective of malicious nodes. Cryptography needs keys for encryption and decryption, each node enters into the network is provided with the unique key. Hence for large networks, the generation of a key becomes complex and consumes more space with the requirement of more hardware, which in turn increase the power consumption. Hybrid cryptographic techniques such as elliptic cryptography, digital signatures, and a combination of symmetric and asymmetric cryptography techniques are also employed to provide security. However, these techniques may not be efficient in WSNs as the complexity increases when a huge network is considered [3–5].

In the proposed approach, convolutional codes are used to generate a security code at multiple hops, which must be matched by the node that wants to access the data. The generation of security code can be discussed as follows:

i. Select the initial security bits as per the network requirement.
ii. By using the convolutional code generator the final security code is obtained by performing EX-OR operation on the initial security bits (as per the convolutional code generation technique).

The IPV4 header is used to store the proposed mathematical technique in the security section comprising 32 bytes. At each hop, different security codes are generated so that the malicious node will not be able to crack the generated code before time to live (TTL), where TTL is the active period of data packets in the link beyond which the data packets are dropped or retransmitted to a legitimate node within the given TTL. Therefore malicious nodes can be easily detected using the proposed technique. This method is simple and less complex and is efficient compared to the key distribution approaches. The remainder of this paper is organized as follows: "Related work" section presents related work, "Proposed approach" section includes a discussion on the proposed approach, "Simulation results" section presents the simulation results, and "Conclusion" section concludes the paper.

Related work

Perrig et al. [3] presented a discussion on the combination of two security protocols to secure sensor networks and improve confidentiality and authentication between the sender and the receiver. But merging two protocols can combine the effects of the demerits of each protocol. Murat [4] analyzed the different protocols used to secure wireless sensor networks from attackers. The author also presented various encryption methods and discussed several attacks and secure network requirements. Necla and Ismail [5] proposed a security technique that combines the Scalable Encryption and Cipher Block Chaining-Message Authentication Code algorithms to ensure dynamic security in the network. However, if the number of transmitted bits increases, power consumption also increases in the network. Chan et al. [6] presented an approach in

which a pair-wise random key is distributed among the nodes to ensure confidentiality in communications. However, pre-distribution of the key itself requires an establishment of trust on the node to which the key is given.

Sathees and Balasubadra [7] presented a discussion on an end-to-end secure method that uses location information to prevent attacks from adversaries, secure routes from source to destination, and increase network lifetime by employing hierarchy routing. Ranjeetha et al. [8] proposed a zone routing model for securing mobile ad-hoc networks by using key distribution. However, key distribution in such networks can be complex because of the lack of central authority. A secure method of data transmission from source to destination is presented in [9], which uses a binary hex residue technique. This method prevents various attacks in mobile ad-hoc networks. Jiye et al. [10] presented an approach in which a session key is employed instead of assigning a permanent key to users of network clusters through Elliptic Curve Diffie–Hellman (ECDH).

Du et al. [11] presented a discussion on time synchronization security techniques that employ high end-sensors in heterogeneous networks. Guo and Shen [12] presented a discussion on a rekeying algorithm, which is pair-wise and is used to ensure the forward and backward privacy of data. In [13], security in WSNs is provided based on the pre-distribution of keys among the nodes that are collaborative. However, cooperation among the nodes may not be possible as the networks are autonomous. Zang et al. [14] proposed an approach for managing keys in hierarchical networks by providing session keys to cluster heads, base stations, and cluster nodes instead of using a common key to secure such networks. Zhengwang et al. [15] proposed a model in which security is provided against malicious attacks by using a dynamic trust. The dynamic trust is determined by the weights of the direct and indirect trusts and uses a sliding window to improve flexibility. However, updating the parameters on a regular basis may be problematic.

Imad et al. [16] presented an approach in which trust among the nodes is established based on the trust factors of the nodes in the network. This trust is established on the records of the nodes, which are used for successful data transmission. However, the node energy is reduced each time the trust participates as a router for transferring information. Padmaja and Marutheswar [17] presented a discussion on the comparative analysis of various methods for detecting malicious nodes and for securing data transmission. Noor et al. [18] developed an energy efficient method of providing security to the network by using the secondary gateway and secondary routing in cluster networks. However, clustering may be difficult in the autonomous structure of networks. An optimized algorithm that is energy efficient is used to improve the trust, prevent attacks on the network, and improve performance [19]. Li et al. [20] developed a localization method for detecting various attacks on WSNs and for minimizing overhead. Kaur et al. [21] presented a secure key distribution method based on a node to node interactions and segregated the attacker nodes to obtain a secure route from source to destination. However, this approach fails when bursts of malicious nodes enter the network at any time interval and mask themselves as active nodes. All the existing approaches use key distribution techniques to secure the data transfer. Key distribution is not efficient as it consumes more energy and storage space to generate the encryption pin and store the decryption pin. Each node entering into the network is provided with these pins therefore for large networks it becomes more complex and more

storage space is required which is limited. In the proposed approach an encoding technique is used to secure the network as it is already available in all the digital communication systems and does not require any additional hardware and different codes are generated at different hops and there is no complexity in key distribution and power consumption is comparatively low because ex-or gates are used to generate the security codes. Hence the proposed approach is applicable for heterogeneous multi-hop networks.

Proposed approach

In this approach, a security code is generated based on the digital encoding technique (i.e. Convolution Coding Approach). Initially, security bits can be selected based on the network requirement. After selecting the security bits the application of the convolutional code is used to finalize the security code word by the use of EX-OR operation on the initial security bits (see Eqs. 2, 3, 4). Table 1 represents the notations used in the proposed approach.

Our approach presents a security model known as the convolutional technique (CT). The security code is obtained by using the convolutional method for preventing malicious attacks against WSNs. In this paper, a 6-bit code is generated at each hop, depending on the initial security bits. The initial security bits 'I_{SC}' is expressed as

$$I_{SC} = H_C - 1, \tag{1}$$

where H_C is Cth hop count and

$$C = 1, 2, 3 \ldots\ldots\ldots\ldots$$

if the hop count is 1 then

$$\begin{aligned} I_{SC} &= H_C - 1 \\ &= 1 - 1 = 0. \end{aligned}$$

As the convolutional technique is presented as a digital method, '0' can be represented as a 3-bit binary number system (because a 3-bit convolutional code generator is used). Therefore I_{SC} can be expressed as

$$\begin{aligned} I_{SC} &= S_{1C} S_{2C} S_{3C} \\ I_{S1} &= S_{11} S_{21} S_{31} = 0\ 0\ 0 \end{aligned}$$

If the hop count is 2 then $I_{S2} = 1$

$$S_{12} S_{22} S_{32} = 0\ 0\ 1$$

Table 1 Notations

I_{SC}	3-bits initial security code
H_c	Cth hop count
S_{1c}, S_{2c}, S_{3c}	Three bits of I_{SC} at Cth hop
G_{1c}, G_{2c}, G_{3c}	Generated bits at Cth hop
C_B	Final security code
N	Total number of initial security bits
M_j	Active nodes
A_j	Attacker nodes
T_N	Source node
R_N	Destination node
T_h	Total number of hops

And if the hop count is 3 then $I_{S3}=2$

$S_{11}S_{21}S_{31} = 0\ 1\ 0.$

In this paper, a three-bit convolutional code generator is used for simplicity and ease of describing the proposed technique (refer to Fig. 1). The equations G_{1C}, G_{2C}, and G_{3C} are obtained using the modulo 2 addition of the initial security bits and are expressed as follows

$$G_{1C} = S_{1C} \oplus S_{2C} \tag{2}$$

$$G_{2C} = S_{1C} \tag{3}$$

$$G_{3C} = S_{1C} \oplus S_{2C} \oplus S_{3C} \tag{4}$$

where S_{1C}, S_{2C}, S_{3C} are the initial security bits at the Cth hop andG_{1C}, G_{2C}, G_{3C} are the generated bits at the Cth hop.

For hop 1, the initial security bits are $S_{11}S_{21}S_{31}=0\ 0\ 0$ and the generated bits are G_{11} $G_{21}G_{31}=0\ 0\ 0$; therefore, the six bits of the security code used to analyze the trust of a node is a concatenation of the initial security bits and the generated bits, which are denoted by C_B

$$C_B = \prod_{i=1}^{N} S_{\mathrm{iC}} G_{\mathrm{iC}} \tag{5}$$

where $S_{iC}G_{iC}$ are placed in a concatenation series and N is the total number of initial bits considered (here $N=3$).

Therefore, at hop 1, $C_B=S_{11}S_{21}S_{31}G_{11}G_{21}G_{31}=0\ 0\ 0\ 0\ 0\ 0$. This method continues until the destination node is reached in the network. Each node in the routing process is verified for the respective C_B, and if it is matched with the security code word expressed in Eq. 5 within the defined TTL, then the data is transmitted to that particular node or the node is considered an attacker node.

Evaluation of proposed method at different hops

Consider a network (refer Fig. 2) with active nodes (M_j) and attacker nodes (A_j), where T_N is the source node, R_N is the destination node, and $j=1,2,3,\ldots\ldots$ indicates the node number. Let T_N communicate with R_N through intermediate nodes M_j. In this paper, the IPV4 header is used by the active nodes to access the data and security operations from source to destination as per the designed algorithm.

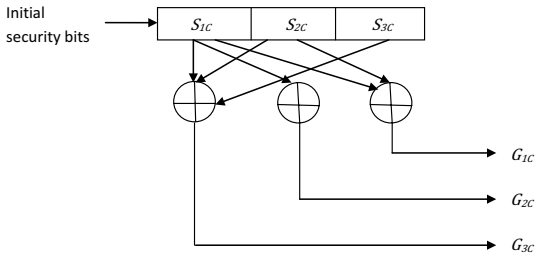

Fig. 1 Block diagram of CT code generator

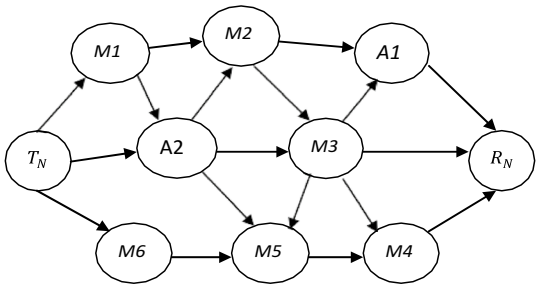

Fig. 2 Example network for evaluating CT

The source node broadcasts the data, including security information, to all its neighboring nodes and if the node is legitimate, it can access the data and again broadcast the data to its neighboring node for further processing. This process continues until the destination node is reached. If the node is malicious, it will not have access to the data because the security operation is unknown to it and would not be able to generate the security code (C_B) within the TTL as the length of the security code is 6 bits and it requires 2^6 combinations, making it a complex process.

The proposed approach is evaluated at multiple hops as

At hop 1

The initial security bits are $S_{11}S_{21}S_{31}=0\,0\,0$ and

G_{11}, G_{21} and G_{31} can be calculated as

$$\begin{aligned} G_{11} &= S_{11} \oplus S_{21} \qquad \text{(from Eq. 2)} \\ &= 0 \oplus 0 \end{aligned}$$

$$\begin{aligned} &G_{11} = 0 \\ &G_{21} = S_{11} = 0 \qquad \text{(from Eq. 3)} \\ &G_{31} = S_{11} \oplus S_{21} \oplus S_{31} \qquad \text{(from Eq.4)} \\ &\quad = 0 \oplus 0 \oplus 0 \\ &G_{31} = 0. \end{aligned}$$

The 6-bit security code $C_B=0\,0\,0\,0\,0\,0$. If this code is matched with a node, then the data can be accessed by that particular node. If C_B is not matched within the TTL, then the node is considered as a malicious node.

At hop 2

The initial security bits are 0 0 1 from (Eq. 1) and

$$\begin{aligned} &G_{12} = S_{12} \oplus S_{22} = 0 \\ &G_{22} = S_{12} = 0 \\ &G_{32} = S_{11} \oplus S_{21} \oplus S_{31} = 1. \end{aligned}$$

Therefore the 6-bit code at hop 2 is $C_B=0\,0\,1\,0\,0\,1$.

At hop 3

The initial security bits are 0 1 0 from (Eq. 1) and

$$G_{12} = S_{13} \oplus S_{23} = 1$$
$$G_{22} = S_{13} = 0$$
$$G_{32} = S_{11} \oplus S_{21} \oplus S_{31} = 1.$$

Therefore the 6-bit code at hop 3 is C_B=0 1 0 1 0 1. In a similar fashion, different codes are obtained at each hop depending on the initial security bits. Table 2 illustrates the 6-bit code with 8 hops.

Because the initial security bits are 3, the total hops covered are $2^3=8$. In general, if the initial security bits are '*N*', then the total number of hops covered can be expressed as

$$T_h = 2^{\mathrm{N}} \tag{6}$$

where T_{h} are the total number of hops covered and '*N*' is the number of initial security bits, $a \geq 3$ (minimum condition). However the selection of '*N*' is user defined, and the user can select the initial security bit number according to the network.

Simulation results

In this section, the simulation results of the proposed approach are discussed in comparison with the Zhang approach [14], Ranjeetha approach [8] and Tao approach [19] as they are fairly recent approaches that provide security to WSNs. MATLAB is used for evaluating the approaches.

The simulation parameters and the required fields related to the size, data, routing, etc. of the network are presented in Table 3. (LAEERP) [22] is used as a routing type. To observe network performance and maintain network dynamicity, pause time is set to 0, 25, 50, 100 ms and the speed of mobility is maintained as 3, 6, 9, 12 m/s.

Figure 3 presents the total number of packets sent by the receiver versus the rate of packet loss. From the figure, it can be observed that the loss rate of packets is comparatively less for the proposed approach as the attacker nodes can be easily detected and removed from the routing path, which minimizes traffic and in-turn reduces the packet loss rate in the network. Figure 4 illustrates the variation in packet overhead in the network in terms of hop count. The packet overhead of the proposed approach is minimal compared to the other three approaches. The complexity of the proposed approach is less because there is no need for key distribution to each node entering the network and updating the key at a regular instance.

Table 2 6-Bit code generation using CT

Hop count (*C*)	S_1	S_2	S_3	G_1	G_2	G_3	C_B
1	0	0	0	0	0	0	000000
2	0	0	1	0	0	1	001001
3	0	1	0	1	0	1	010101
4	0	1	1	1	0	0	011100
5	1	0	0	1	1	1	100111
6	1	0	1	1	1	0	101110
7	1	1	0	0	1	0	110010
8	1	1	1	0	1	1	111011

Table 3 Simulation parameters

Parameters	Considered values
Time for simulation	650 s
Nodes count considered	2 to 120
Maximum hop count	9
Propagation model	Two-ray ground
Type of link layer	Logical link
Type of MAC used	802.11
Type of queue	Drop-tail
Packet size	512 bytes
Routing type	LAEERP
Traffic	Video
Pause time	0, 25, 50, 100 ms
Network area	1000 m × 1000 m
Speed of node	3, 6, 9, 12 m/s

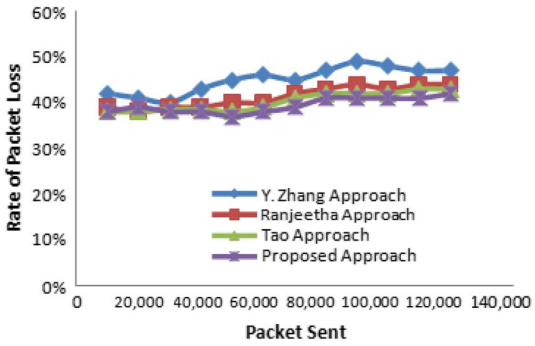

Fig. 3 Packets sent v/s rate of packet loss

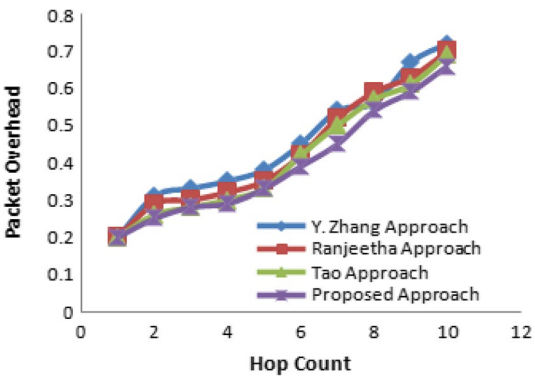

Fig. 4 Hop count v/s packet overhead

Figure 5 presents information on the packet delivery ratio (PDR) at different simulation times. The PDR of the proposed approach is initially almost equal to that of existing approaches as the initial security bits are loaded into S_1, S_2 and S_3. After elapse of time,

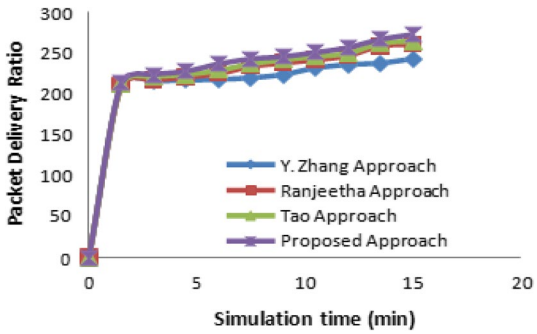

Fig. 5 Simulation time v/s PDR

the PDR of the proposed approach is better when compared to conventional approaches because the malicious nodes are removed from the routing path and packets are delivered with minimal loss.

The proposed approach is quite efficient as it generates the security codes at each hop easily using mathematical operations, unlike the complex key distribution methods. The simulation results of the proposed technique outperform the existing methods as the packet overhead and packet loss is minimal which improves the PDR.

Conclusion

WSNs are precise and consistent in the efficient transfer of data. The proposed approach provides security to such networks through convolutional codes without any key distribution, which consumes more power and storage space. The proposed technique is efficient as it can be generated by simple mathematical equations that reduce computational power and easily detect malicious nodes for secure data transmission from source to destination. The simulation results demonstrate that the proposed approach provides better results compared to conventional approaches, and it is simple and effective for providing security to WSNs.

Declaration

I, the undersigned declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere.

Authors' contributions

A simple and effective convolution technique is developed to enhance trust among nodes in wireless sensor networks. At each hop, a new security code is generated to secure data transmission from source to destination. The author read and approved the final manuscript.

Authors' information

Turki Ali Alghamdi is Associate Professor in Computer Science Department, Faculty of Computer and Information Systems, University of Umm Al-Qura in Makkah, Saudi Arabia. He holds a B.Sc. in computer science He holds a B.Sc. in computer science. He was awarded M.Sc. degree in Distributed Systems and Networks from the University of Hertfordshire, Hatfield in 2006. In 2010 he received his Ph.D. degree in Computer Networks from the University of Bradford, Bradford, United Kingdom. He has previously been Vice Dean of Technical Affairs (IT Deanship) at Umm Al-Qura University in Makkah and Dean of eLearning and IT at Taif university in Taif. He is holder of CDCDP and CDCMP certificates. He is passionate about developing the translational and collaborative interface between industry and academia. Turki's research, focusing on Wireless Sensor Networks, Energy and QoS Aware Routing Protocols, Network Security, IoT and Smart Cities.

Funding

Not applicable.

Availability of data and materials
Not applicable.

Competing interests
The author declares no competing interests.

Received: 20 March 2019 Accepted: 9 October 2019
Published online: 22 October 2019

References

1. Li Y-X, Qin L, Liang Q (2010) Research on wireless sensor network security. In: International conference on computational intelligence and security, pp 493–496
2. Chen X, Makki K, Yen K, Pissinou N (2009) Sensor network security: a survey. IEEE Commun Surv Tutorials 11(2):52–73
3. Perrig A, Szewczyk R, Wen V, Cullar D, Tygar JD (2002) SPINS: security protocols for sensor networks. Int J Commun Comput Inform 8(5):521–534
4. Murat D (2014) Security analysis in wireless sensor networks. Int J Distrib Sens Netw 2014:1–9
5. Necla B, Ismail E (2012) WSNSec: a scalable data link layer security protocol forWSNs. Ad Hoc Netw 10(1):37–45
6. Chen H, Perrig A, Song D (2003) Random Key Predistribution Schemes for Sensor Networks, Proceedings of the 2003 IEEE symposium on security and privacy, pp 197–213
7. Sathees S, Balasubadra K (2018) Chronic privacy protection from source to sink in sensor network routing. Int J Appl Eng Res 13(5):2798–2808
8. Ranjeetha S, Renuga N, Sharmila R (2017) Secure zone routing protocol for MANET. In: International conference on emerging trends in engineering, science and sustainable technology (ICETSST-2017), pp 67–76
9. Ahmad SJ, Radha Krishna P (2018) BHQRSM: binary hex quadratic residue security model to enhance the trust in MANETs. Wireless Pers Commun 101(2):661–676
10. Jiye K, Moon J, Jung J, Won D (2016) Security analysis and improvements of session key establishment for clustered sensor networks. Hindawi Publish Corp J Sens 2016:1–17
11. Du X, Guizani M, Xiao Y, Chen H-H (2008) Secure and efficient time synchronization in heterogeneous sensor networks. IEEE Trans Vehic Tech 57(4):2387–2394
12. Guo S, Shen AN (2010) A compromise-resilient pair-wise rekeying protocol in hierarchical wireless sensor networks. Comput Syst Sci Eng 25(6):397–405
13. Zhang W, Zhu S, Cao G (2009) Pre distribution and local collaboration-based group rekeying for wireless sensor networks. Ad Hoc Netw 7(6):1229–1242
14. Zhang Y, Wu C, Cao J, Li X (2013) A secret sharing-based key management in a hierarchical wireless sensor network. Int J Distrib Sens Netw 2013:1–7
15. Zhengwang Y, Wen T, Song X, Liu Z, Fu C (2017) An efficient dynamic trust evaluation model for wireless sensor networks. J Sens 2017:1–16. https://doi.org/10.1155/2017/7864671
16. Imad J, Mohammed F, Jaroodi JA, Mohamed N (2016) TRAS: a trust-based routing protocol for ad hoc and sensor networks. In: IEEE 2nd international conference on big data security on cloud, IEEE international conference on high performance and smart computing, IEEE international conference on intelligent data and security, pp 382–387
17. Padmaja, Marutheswar GV (2017) Detection of malicious node in wireless sensor network. In: Proceedings on IEEE advanced computer conference (IACC), pp 193–198
18. Noor Z, Jung L, Alsaadi F, Alghamdi T (2012) Wireless sensor network (WSN) routing security, reliability and energy efficiency. J Appl Sci 12:593–59
19. Tao Y, Xiangyang X, Tonghui L, Leina P (2018) A secure routing of wireless sensor networks based on trust evaluation model. Procedia Comput Sci 131(2018):1156–1163
20. Li P, Xiaotian Yu, He X, Jiewei Qian L, Dong HN (2017) Research on Secure Localization Model Based on Trust Valuation in Wireless Sensor Networks. Security and Communication. Networks 2017:1–12. https://doi.org/10.1155/2017/6102780
21. Kaur J, Gill SS, Dhaliwal BS (2016) Secure trust based key management routing framework for wireless sensor networks. J Eng 2016:1–9. https://doi.org/10.1155/2016/2089714
22. Ahmad SJ, Damodaram A, Reddy VSK, Krishna PR (2013) Location aware and energy efficient routing protocol for long distance MANETs. Int J Netw Virtual Organ 13(4):327–349

Publisher's Note