Alotaibi *EURASIP Journal on Wireless Communications and Networking* (2019) 2019:8
https://doi.org/10.1186/s13638-018-1337-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Security to wireless sensor networks against malicious attacks using Hamming residue method

Majid Alotaibi

Abstract

Wireless sensor networks (WSNs) consist of small sensor nodes with limited energy. Such nodes have the ability to monitor the physical conditions and communicate information among the nodes without the requirement of the physical medium. WSNs are autonomous and are distributed in space. Due to the absence of central authority and random deployment of nodes in the network, WSN is prone to security threats. Well-known attacks in WSN are a malicious attack (such as compromised node imitating as one of the network nodes, misleading other nodes). In the art of work, various methods are developed to overcome these attacks either by cryptographic approaches or by time synchronization. But these methods may fail because of WSN autonomous structure. In this paper, an efficient approach called Hamming residue method (HRM) is presented to mitigate the malicious attacks. The experimental results validate the presented approach.

Keywords: WSN, Malicious attacks, Rival nodes, PDR, NS2, Hamming residue method

1 Introduction

Wireless sensor networks have self-dependent sensor nodes distributed in the space which are easily deployable in adverse conditions to monitor the environmental conditions such as noise, temperature, and pressure. These nodes are capable of transferring the data from one node to another without any physical medium. To transfer the data from source to destination, the source node can directly interact with the destination node or may interact with the router nodes which act as an interface between source and destination nodes. Such network with router nodes is known as multi-hop networks. WSN provides a gateway which acts as an interface between end user to process the data transmitted by the sensor nodes. Such type of networks poses some limitations. As the nodes are widely spread, WSNs are exposed to various malicious attacks such as the malicious node can easily enter into the network and the rival node masked as one of the network nodes, misguiding the other nodes present in the network and network congestion. Due to a huge number of nodes present in WSN, security must be given at different levels, which is complicated.

In the art of work, the research provides different approaches to secure the communication in WSN. Cryptography is one of the common solutions for providing security. In this method, the key is distributed among the nodes either in symmetric or in asymmetric fashion. However, the asymmetric distribution of key requires more cost with less speed. In symmetric key distribution, key distribution is complicated as the key should be transmitted before the message. So, to reduce the complexity and eliminate the key distribution among the nodes, a simple and effective method is proposed which is called the Hamming residue method (HRM). The proposed technique enhances the security of the network against malicious attacks and improves the efficiency of the network. In this approach initially, a codeword is being generated by the use of defined initial security bits (user choice) and security check bits (Hamming bits). After which, quadratic residue technique is being employed to enhance the security at various hops. Using IPV6, the information regarding the HRM is stored in the header and if the code matches with the code generated by the intermediate node, then it can access the

Correspondence: mmgethami@uqu.edu.sa
Department of Computer Engineering, College of Computer and Information Systems, Umm Al Qura University, Makkah, Saudi Arabia

data; if not, the node is considered to be an attacker node.

The rest of the paper is organized as follows: Section 2 gives the methodology of the presented approach; in Section 3, related work is presented; the proposed approach is discussed in Section 4; Section 5 presents the simulation results; and conclusion is being presented in Section 6.

2 Method

In the presented approach, an efficient security methodology is proposed by the implementation of Hamming residue method. For simplicity, Hamming code as (7, 4) is chosen along with the quadratic residues of 7 to improvise the security. However, one can choose any Hamming code and residues based on the network requirements. The entire technique is stored in IPV6 packet header such that all the non-malicious nodes will produce the security code within the specified time to live (TTL). However, it will take more time than TTL for malicious nodes to analyze the security code generation technique. Hence, this method can easily detect the rival node, improving the packet delivery ratio (PDR) and reducing the delay in the network. This method provides the security to WSNs against the malicious attacks without any key distribution mechanism.

3 Related work

WSNs have several security issues; the present literature addresses these issues with different models and techniques. Various attacks in the sensor networks, their remedial measures, and future perspective are discussed in [1, 2]. Roberto et al. [3] proposed a beneficial method to mitigate simple attacks in WSN. It mainly concentrates on unattended WSNs (UWSNs) in which the central authority is not present for long time periods. Laurent and Virgil [4] presented an approach in which the key is distributed by using random probability.

Delay attacks in WSN can be avoided with the help of two methods given by Song et al. [5], one is generalized extreme Studentized deviate (GESD) algorithm to detect the malicious node and the other is based on preset value to filter out such nodes. The method proposed by Tao et al. [6] mainly focuses on the compromised node and DoS attack by designing multi-path random routing algorithm. The approach presented by Xiaojiang et al. [7] discusses an effective security technique for cooperative sensing nodes by time synchronization using the strength of high end sensors. But cooperation between the nodes may be difficult due to lack of centralized authority. In [8–10], the authors discuss confidential key sharing methods to establish a session of communication in the network and to avoid problems caused by the compromised node.

Sengar and Bhardwaj [11] discussed applications of WSN and various attacks (such as active and passive attacks) incorporated with it. They also discuss the importance of trust and fairness of the data transferred from source to destination. The approach proposed by Tang et al. [12] presents a secure routing algorithm with a selection of the shortest path and deterministic strategies to normalize the power consumption, and supports different routing methods to secure the data. However, this strategy may fail as the energy of the node is not considered which is the main constraint in WSNs. Rashmi and Archana [13] proposed a model in which dynamic multi-level priority (DMP) for scheduling the packets with bit rate categorization and Rivest cipher 6 (RC6) algorithm is used for providing security to WSN.

The approach presented by Jiye Kim [14] develops a session key concept for cluster networks by using elliptic curve Diffie-Hellman (ECDH) for exchanging the keys, and improves the security in WSNs. A method presented by Pawani et al. [15] discusses a keying technique for the Internet of Things (IoT) applications in WSNs. They developed a PAuthkey to provide secured channels to the end users. However, the distribution of key itself is a complex task as the network is dynamic in nature. In the presented approach, Hamming residue model is used to secure the WSNs from the malicious attacks. The rival nodes causing such attacks can be easily detected and are removed from the network. Jalal et al. presented [16] to secure the MANET using block coding; however, the presented approach is very much complex and increases delay, which in turn decreases PDR.

4 Proposed approach

In digital communication, Hamming codes are used to detect and correct the errors; as a result, all the communication systems are aware of these codes. WSNs are autonomous and require less energy consumption, and such codes can be used to secure WSN system without any additional infrastructure. In the presented approach, initial security bits (users define) are used and a set of additional security check bits is appended to it for generating the security codeword. Depending on the security codeword length "n" and a number of initial security bits "k," Hamming codes (n, k) (such as (6, 3) and (7, 4) codes) can be used or many more. The security codeword "W" is obtained by appending $n - k$ security check bits "SC" to the initial security bits "S" (refer to Eq. 1)

$$\begin{aligned} W &= W_1..W_2..W_3...W_n \\ &= S_1..S_2..S_3...S_kSC_1..SC_2..SC_3...SC_p \end{aligned} \quad (1)$$

where $p = n - k$
"S_i" is ith bit of "S," i = 1, 2, 3.... k
"SC_j" is jth bit of "SC," j = 1, 2, 3... p

"W_m" is mth bit of "W," $m = 1, 2, 3... n$

If the number of initial security bits is k, then the possible initial security bits matrix block "S_B" is represented as

$$S_B = \begin{pmatrix} S_{11} & S_{12} \cdot \cdots S_{1k} \\ S_{21} & S_{22} \cdot \cdots S_{2k} \\ \cdots\cdots\cdots\cdots\cdots \\ S_{q1} & S_{q2} \cdot \cdots S_{qk} \end{pmatrix} \quad (2)$$

where S_{ab} represents the element of ath row and bth column, $q = 2^k$ = total number of rows, and k = total number of columns in S_B.

In this approach, (7, 4) Hamming code is used to generate the security codeword "W." However, one can select the Hamming code according to the desired initial security bits and security codeword length. Here, initial security bits are 4 and the possible initial security bits matrix block is (i.e., 0–15 represented in binary bits)

$$S_B = \begin{pmatrix} 0\ 0\ 0\ 0 \\ 0\ 00\ 1 \\ 0\ 01\ 0 \\ \cdots\cdots \\ 1\ 1\ 11 \end{pmatrix} \quad (3)$$

Here, in the presented approach, the initial security bits at source node are 0 0 0 0 (i.e., hop 0), so at hop 1, security bits are 0 0 0 1 so on till hop 15 as the proposed approach is designed up to 15 hops only. Thus, simply one can say that the initial security bits are binary equivalent of hop number.

Initial Security bits = hop number (represented in a binary system)

After obtaining the initial security bits, the security check bits are added to them. These check bits are generated by multiplying and performing modulo 2 additions of the initial security bits with the security matrix as represented in Eq. 4

$$SC = S \times SP_m \quad (4)$$

where SP_m is $(k \times p)$ security matrix represented as

$$SP_m = \begin{pmatrix} l_{11} & l_{12} & \cdots l_{1p} \\ l_{21} & l_{22} \cdot \cdots l_{2p} \\ \cdots\cdots\cdots\cdots\cdots \\ L_{k1} & l_{k2} \cdot \cdots k_{kp} \end{pmatrix} \quad (5)$$

where "l_{rf}" represents the element of rth row and fth column.

The security matrix is the parity matrix of (7, 4) Hamming code which is obtained either from its parity check matrix or from its generator matrix. These two matrices are already defined for the Hamming codes. In the

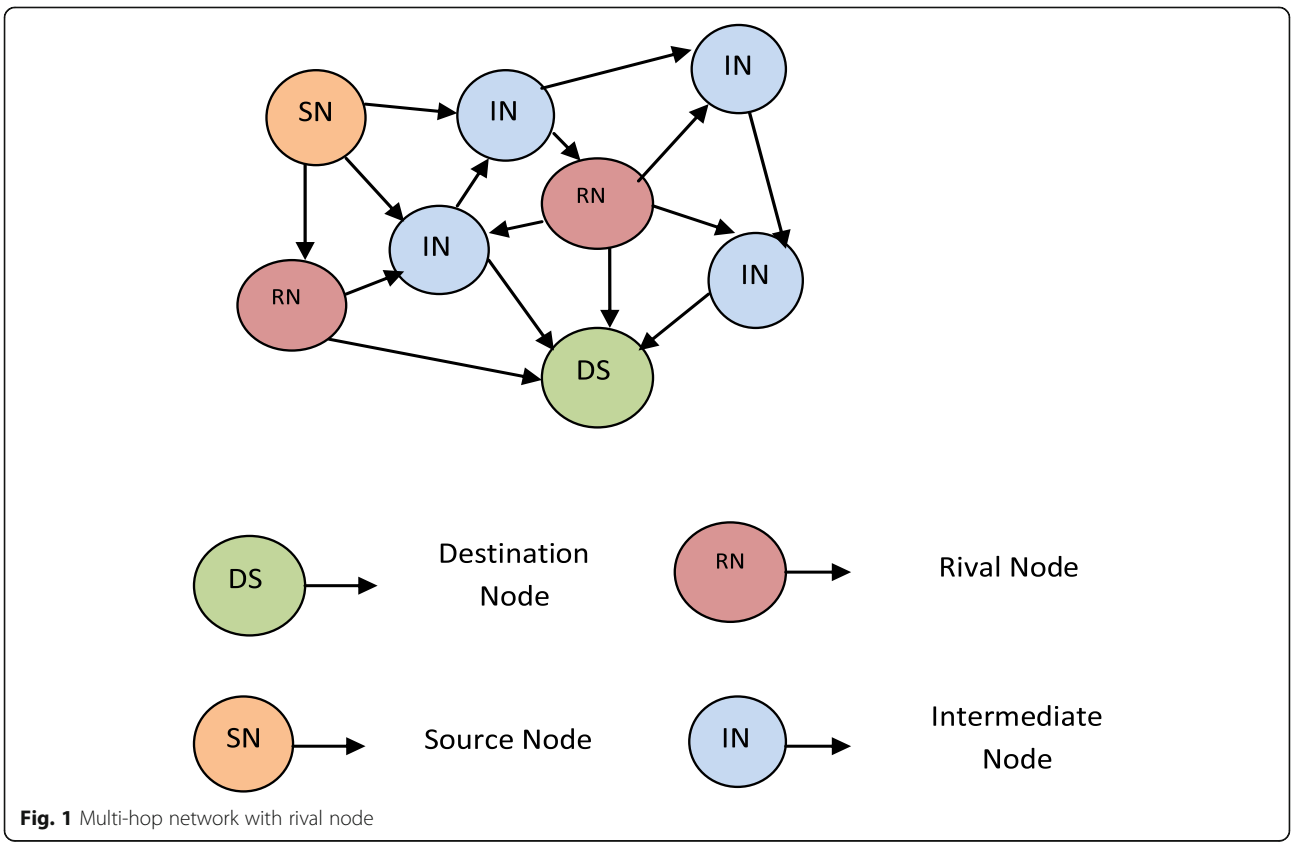

Fig. 1 Multi-hop network with rival node

presented model, the SP_m is common to all the source nodes in the network and is defined as

$$SP_m = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

For example, at source node, the initial security bits are (0 0 0 0); hence, the security check bits are

$$SC_{h0} = S_{h0} \times SP_m = [0 \quad 0 \quad 0 \quad 0] \times \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$= (0 \quad 0 \; 0)$$

where SC_{hr} are the check bits at rth hop

S_{hr} are the security bits at rth hop, $r = 0, 1, 2, 3$ ....

Hence, the security codeword at the source node is obtained by appending SC_0 to the security bits of the source node and can be represented as

$$W_{h0} = S_1 \; S_2 \; S_3 \; S_4 \; C_1 \; C_2 \; S_3 = 0 \; 0 \; 00 \; 0 \; 0 \; 0$$

where W_r is the security codeword at hop r, $r = 0, 1, 2,$....

After evaluating the security codeword, the quadratic residue is used to provide additional security as only Hamming codes may not be efficient to provide the desired security to WSNs. Quadratic residues are user-defined, secure, easy to implement, and are readily available. In this approach, the residue of 7 is considered, as the length of security codeword obtained is 7 and covers maximum bits in the security codeword to enhance the security. Residues of 7 are 1, 2, and 4; here, in the presented approach, these bit positions (i.e., 1, 2, and 4) are complemented in the codeword. So, the generated final security codeword can be represented as

$$R_{w0} = 1 \quad 10 \; 1 \; 0 \; 00$$

where "R_{w0}" is the final security codeword (after complementing residue positions in W_0) at the rth hop. Apart from synchronization of the final security codeword, the packet delivery ratio (PDR) (see Eq. 6) of the nodes is continuously being monitored. If PDR value is

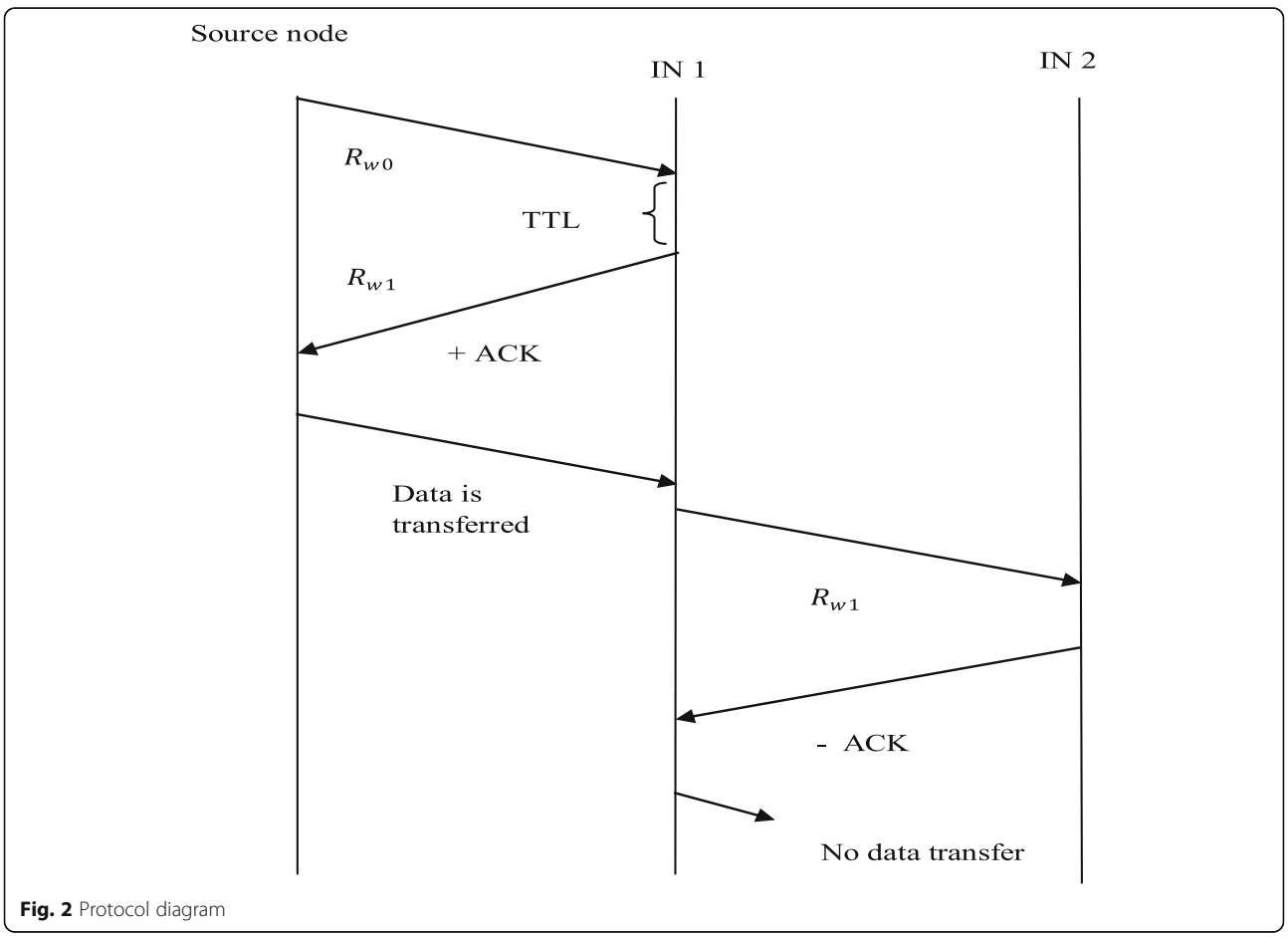

Fig. 2 Protocol diagram

acceptable, only then that the data is transferred, and if it is beyond the acceptable limit, data is not passed further. In similar fashion, this process continues until the destination node.

$$\text{PDR} = \text{No.of R.P/No.of T.P} \quad (6)$$

where R.P is the received packets and T.P is the transmitted packets

4.1 Node matching process

Figure 1 depicts a multi-hop network in which the source node communicates with the destination node through intermediate nodes. The source node sends R_{w0} to all its neighboring nodes which are one hop away from the source node. The required operation at various hops is discussed in Sections 4.1.1 and 4.1.2.

4.1.1 At hop 1

The initial security bits are 0 0 0 1; the security check bits are generated by multiplying these bits with

$$\begin{aligned} C_{h1} &= S_{h1} \times SP_m \\ &= (1 \quad 0 \quad 1) \end{aligned}$$

And the codeword at hop 1 can be evaluated as below

$$W_{h1} = 0 \quad 0 \; 0 \; 1 \quad 1 \; 0 \; 1$$

Complementing the residue (of 7) positions (i.e., first, second, and fourth positions) in $Wh1$, the final security codeword at hop 1 is represented as

$$R_{w1} = 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1$$

If the neighboring node sends $Rw1$ as an acknowledgement to the source node and its PDR value is acceptable, then the source node will transfer the original data to that neighboring node. The acknowledgement should not exceed the provided time to live (TTL). Now, this neighboring node becomes the source node for other nodes in the network and transmits $Rw1$ to its neighboring nodes.

Table 1 Parameters for simulation

Parameters	Values
Node count	2 to 150
Simulation period	70 s
Layer	Logical link
Antenna used	Omni directional
Type of queue	Drop tail
MAC	802.11
Data	VBR

4.1.2 At hop 2

The security bits are 0 0 1 0, and the check bits are

$$\begin{aligned} C_{h2} &= S_{h2} \times SP_m \\ &= (1 \quad 1 \quad 1) \end{aligned}$$

$$W_{h2} = 0 \quad 0 \; 1 \; 0 \quad 1 \quad 1 \quad 1$$

Complementing the residue positions in $Wh2$, the final security codeword at hop 2 can be calculated as

$$R_{w2} = 1 \; 1 \; 1 \; 1 \; 1 \; 1 \; 1$$

If the source node is acknowledged with $Rw2$, then it will pass the data to the node from which it has received the acknowledgement. If not, the node is considered to be a rival node and the data is not transmitted to that

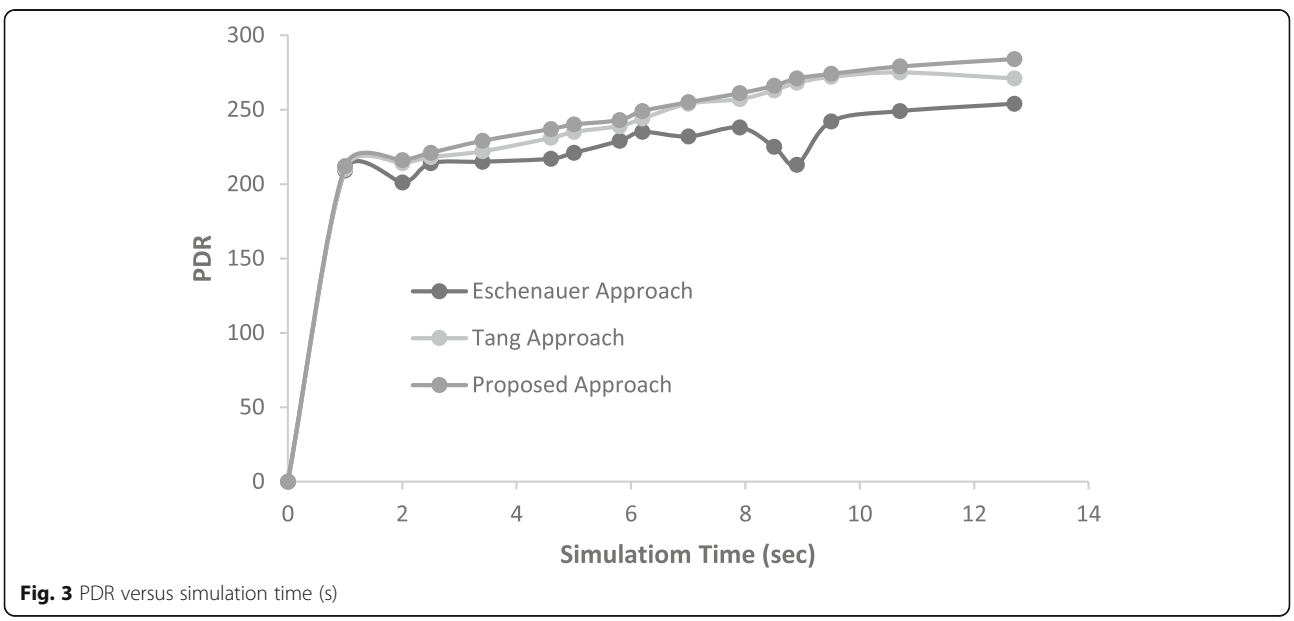

Fig. 3 PDR versus simulation time (s)

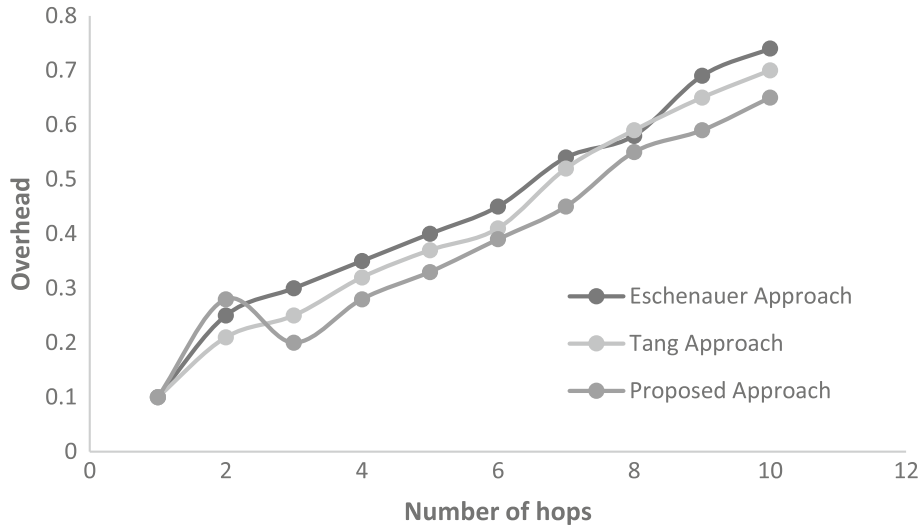

Fig. 4 Overhead versus number of hops

node. This process is continued till the information or data is received by the destination node. This process can be easily understood by using protocol diagram (see Fig. 2). As the security codeword is changed at every hop and becomes very difficult to the rival nodes to mislead the active node in the network, so the presented approach not only improves the authentication of the active node but also gives more confidentiality to end nodes by designing multiple codewords in the network. From Fig. 2, it is observed that the data is transferred to intermediate node 1 (IN1) from the source node as it gives the positive acknowledgment (+ACK), i.e., 1, to the source node. Once the data is received by IN1, it acts as the source node for its neighboring nodes and transmits 1 to them. The data is not transferred to intermediate node 2 (IN 2) as it gives negative acknowledgement (−ACK) to IN1, hence considered to be a rival node.

5 Simulation results

The presented approach is validated by simulating the results using Network Simulator 2 (NS2) [17] and comparing this approach with the approach that already exists. Table 1 represents different parameters which are considered for simulation. The node count is taken between the range of 2 and 150; however, by the use of Hamming code (7, 4), the maximum number of nodes possible is 15.

Figure 3 gives the variation of packet delivery ratio (PDR) with respect to the simulation time. The presented approach shows the better result when compared with Eschenauer's approach [4] which is a moderate recent research work and Tang's approach [12] which is the very recent research work. Initially, the PDR of the presented approach is approximately equal to that of Tangs's approach but as the simulation time is increased the PDR increases. Figure 4 gives the relation between overhead and the number of hops; it is observed that overhead of the proposed approach is less when compared with the other two approaches, though the graphs vary slightly when compared to the other two methods but have a significant effect on the data transfer. The acceptable limits for video and audio packets are 150 ms and 400 ms respectively [18]. The proposed approach is valid up to 15 hops as the example of (7, 4) Hamming code is presented. However, the number of hops can be increased by increasing their initial security bits length and security codeword length as per the Hamming code.

6 Conclusion

The security of wireless sensor networks is improved by the Hamming residue technique. The presented approach is simple and very much effective if more number of rival nodes exists at different hops in the network. As at each node, a new security codeword is generated, which makes the proposed method more efficient, enhances the confidentiality among the nodes, and can easily detect the rival node in the network. The presented approach also reduces the mathematical complexity which in turn increases the PDR by minimizing the delay.

Abbreviations

−ACK: Negative acknowledgement; +ACK: Positive acknowledgement; DMP: Dynamic multi-level priority; ECDH: Elliptic curve Diffie-Hellman; GESD: Generalized extreme Studentized deviate; HRM: Hamming residue method; IN1: Intermediate node 1; IoT: Internet of Things; MAC: Medium access control; NS2: Network Simulator 2; PDR: Packet delivery ratio; RC6: Rivest cipher 6; TTL: Time to live; UWSNs: Unattended wireless sensor networks; WSNs: Wireless sensor networks

Acknowledgements
Not applicable

Funding
Not applicable

Availability of data and materials
Open access

Author's contributions
An efficiently secure technique is proposed to secure the wireless sensor networks from the malicious attacks by using the Hamming residue method. The author read and approved the final manuscript.

Author's information
Majid Alotaibi received Ph.D., from The University of Queensland, Brisbane, Australia, in 2011. Currently, he is an assistant professor with the Department of Computer Engineering, Umm Al Qura University, Makkah, Kingdom of Saudi Arabia. His current research interests include mobile computing, mobile and sensor networks, wireless technologies, ad hoc networks, computer networks (wired/wireless), RFID, antennas and propagation, radar, and nano electronics.

Competing interests
The author declares that there are no competing interests.

Publisher's Note

Received: 26 April 2018 Accepted: 21 December 2018
Published online: 08 January 2019

References

1. C. Karlof D. Wagner Secure Routing in Sensor Networks: Attacks and Countermeasures Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Apps.2003
2. Y. Zhou, Y. Fang, Y. Zhang, Securing wireless sensor networks: a survey. IEEE Commun. Surv. Tutorials. **10**(3) 6–28 (2008)
3. R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, G. Tsudik, Data security in unattended wireless sensor networks. IEEE Trans. Comput. 58(11), 1500–1511 (2009)
4. L. Eschenauer, V.D. Gligor, *A Key Management Scheme for Distributed Sensor Networks*, Proc. 9th ACM Conf. Comp. and Commun (2002), pp. 41–47
5. H. Song S. Zhu G. Cao Attack-Resilient Time Synchronization for Wireless Sensor Networks Proc. 2nd IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Sys. 2005
6. T. Shu, M. Krunz, S. Liu, Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE Trans. Mob. Comput. 9(7), 941–954 (2010)
7. X. Du, Secure and efficient time synchronization in heterogeneous sensor networks. IEEE Trans. Vehic. Tech. 57(4), 2387–2394 (2008)
8. W. Zhang, S. Zhu, G. Cao, Pre-distribution and local collaboration-based group rekeying for wireless sensor networks. Ad Hoc Netw. **7**(6), 1229–1242 (2009)
9. S. Guo, Z. Qian, A compromise-resilient pair-wise rekeying protocol in hierarchical wireless sensor networks. Comput. Syst. Sci. Eng. 25(6), 397–405 (2010)
10. Y. Zhang, C. Wu, J. Cao, X. Li, A secret sharing-based key management in a hierarchical wireless sensor network. Int. J. Distrib. Sens. Netw. 2013(Article ID 406061), 7 (2013)
11. P. Sengar, N. Bhardwaj, A survey on security and various attacks in wireless sensor network. Int. J. Comput. Sci. Eng. 5, 4 (2017)
12. D. Tang, T. Li, J. Ren, J. Wu, Cost-Aware SEcure Routing (CASER) protocol design for wireless sensor networks. IEEE Trans. Parallel. Distributed Syst. 26(4), 960–973 (2015)
13. R. Mahidhar, A. Raut, A survey on scheduling schemes with security in wireless sensor networks. Int. Conf. Inf. Secur. Privacy 78, 756–762 (2016)
14. J. Kim, J. Moon, J. Jung, D. Won, Security analysis and improvements of session key establishment for clustered sensor networks. Hindawi Publishing Corp J Sens 2016, Article ID 4393721, 17 https://doi.org/10.1155/2016/4393721. Accessed 10 Apr 2016
15. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, PAuthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. Int. J. Distrib. Sens. Netw. 2014, Article ID 357430, 14 (2014). https://sourceforge.net/projects/nsnam/
16. Syed Jalal Ahmad and P. Radha Krishna, Security on MANETs using Block Coding. International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp 2054–2060, 2015.
17. NS2 Download link: https://sourceforge.net/projects/nsnam/
18. S.J. Ahmad, V.S.K. Reddy, A. Damodaram, P. Radha Krishna, A dynamic priority based scheduling scheme for multimedia streaming over MANETs to improve QoS. Int. Conf. Distrib. Comput. Internet Tech., 122–126 (2016)