Egyptian Informatics Journal 22 (2021) 119–124

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

AHKM: An improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in IoT

A.B. Feroz Khan [b,*], G. Anandharaj [a]

[a] PG and Research Department of Computer Science, Adhiparasakthi College of Arts and Science (Autonomous), G.B.Nagar, Kalavai-632506, India
[b] Department of Computer Application, C.Abdul Hakeem College of Engineering and Technology, Melvisharam-632509, India

ARTICLE INFO

Article history:
Received 19 February 2020
Revised 23 March 2020
Accepted 18 May 2020
Available online 6 June 2020

Keywords:
IoT
Security
Key management
Cluster-based network

ABSTRACT

The extensive growth of the Internet of Things (IoT) devices leads to the evolution of the broad range of smart applications in numerous fields such as smart home, wearable, education, agriculture, health care, transportation and many more. But security for IoT devices is still a challenging issue as many attacks are possible in the environment. Therefore strong security requirements are an important concern to safeguard the IoT smart devices. The sensor network has to select an efficient encryption algorithm to provide secure communication between sensor nodes. The basic requirement for encrypted communication is key establishment and distribution. The currently available key management process involves large computational overhead, energy consumption, and delay. This makes the network inefficient since sensor nodes have limited bandwidth capacity. The main aim of this paper is to establish a strong key management mechanism to overcome the issues in the current cluster based key management technologies. The work proposed a secure hash key-based key management scheme for the cluster based network environment. The proposed scheme considers the two-level verification process, a one-hop way for the nodes within the cluster and a multi-hop way for the nodes outside the transmission range. The work done is examined through simulation by varying the number of malicious nodes in the environment. The result shows that the rate of packet loss has been reduced when compared with a one-hop way of key management solution. The proposed work also enhances the performance of the network by lowering the energy, computational overheads, and delay.

© 2020 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

IoT is a collection of smart devices where all the devices are having the ability to communicate with each other, they can infer and measure the surroundings through its sensing nature and send the result to the intended node in the environment with the help of the internet. There are many IoT smart applications outspreaded in various fields such as wearable, health, personal care, agriculture, water disaster management, transportation, etc. The security requirements for such applications are crucial to save the network from different security attacks [1]. IoT is prone to many variations of Denial of Service (DoS) attacks, and jamming is one of the DoS attacks, which is considered as the most serious attack on the IoT network. This attack will block the channels and deny providing the service for authorized users and hence the network incurred performance degradation. Even though efficient encryption techniques are available for secure communication of smart devices, the present key management schemes make the network inefficient in terms of large energy consumption, computational overhead, and delay. To protect the environment from security attacks, encryption techniques along with efficient key management strategies are important requirements [2]. This paper proposed a hash key based key management scheme with the multi-hop approach. The hash based security solution is considered to be an efficient solution for smart networks. Most of the sensor networks are deployed with cluster based techniques, which helps increase the efficiency of energy and scalability. Hence cluster based networks using robust cluster based key management techniques should be incorporated to create a highly secure envi-

* Corresponding author.
E-mail addresses: abferozkhan@gmail.com (A.B. Feroz Khan), younganand@gmail.com (G. Anandharaj).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

https://doi.org/10.1016/j.eij.2020.05.004
1110-8665/© 2020 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelligence, Cairo University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

ronment. This work proposes an efficient hash based key management scheme.

The currently available hash based key management schemes [2–7] incurred more computational overheads and they are not suitable for a smart environment such as IoT. This proposed work uses a one-way hash function for the establishment of a secure key between one-hop and multi-hop nodes and the nodes can be communicated through a secured link. Each node in the network has 2 keys: local key and pair-wise key, the local key is distributed to each node by the coordinator node and the pair-wise key is generated within the cluster for single hop nodes and outside the cluster for multi hop nodes. The proposed scheme is compared with one-hop key management schemes [2–7]. The work considers 3 performance measures, energy, delay, and computation cost by increasing the number of malicious nodes in the environment. The outcome of the simulated evaluation shows that the performance of the network is largely increased in the presence of the jamming attack by establishing a secure key between one hop and multi hop path.

The rest of the work is divided into 5 sections. The related work of cluster based key management mechanisms with its merits and demerits are described in Section 2. In Section 3, the proposed cluster hash key based key management for cluster based networks is discussed in detail with its system model. Section 4 provides the simulation results of the proposed scheme by evaluating the network with increased malicious nodes in the environment. Finally, Section 5 concludes the work.

2. Related work

In this section, we discuss the current key management mechanism based on hash-based secret keys in the cluster-based sensor network.

Lin You et al. [2] described a key management scheme for wireless sensor networks, where the work proposed a key distribution scheme using hash chain with deployment knowledge (DKH-KD). It established a pairwise key based on the number of hash chains. The pairwise key was established through reverse hash chain values. It improves the establishment of pairwise key more efficiently but computational cost is significantly increased with the rekeying process.

Shuang Jia et al. [3] proposed an effective and lightweight Authentication and Key Management Scheme (AKMS) to lower the computational cost required in the key generation process. The computational overhead occurred due to the increased number of malicious nodes in the sensor network. The proposed work improves the security of the network and reduces the computational overheads incurred.

Ehdai et al. [4] described a 2D hash-based scheme, where the author used two hash functions to solve the security issues in the sensor network and it works efficiently against node capture attack. The work greatly reduces the energy consumption but computation overhead increased due to the rekeying process.

Ahlawat et al. [5] proposed a Hybrid Approach for Path Vulnerability Matrix on Random Key Pre-distribution for Wireless Sensor Networks which uses a random pre-distribution key that lowers the energy consumption and decreases the node capture attack.

Priyanka et al. [6] introduced an attack model based highly secure key management scheme for wireless sensor networks which reduces the node capture attack by creating a hash chain. The hash chain created is based on the security requirement of each cell in the network. The security required for each cell is measured by analyzing the compromised probability of each cell. The proposed work highly enhance the security of the network but the computational cost increased due to a large number of rekeying process.

Anita et al. [7] described a novel hybrid key management scheme for establishing secure communication in wireless sensor networks which decreases the computational overheads and guaranteed high-level security over communication networks. The work shows that the performance of the network is enhanced but it is difficult to implement in real-time situations.

Table 1 shows the background work of different hash-based key management schemes for the enhancement of security against malicious nodes in the network. The table list out the proposed scheme used with its merits and demerits. The main drawbacks of the schemes are that they all used one hop distance for the secure link, which needs to be established between sensor nodes and are not highly scalable with the large sized network and not suitable in real time scenarios. Another important drawbacks of all the work discussed are: they are not scalable and hence they could not cope up with a dynamic environment that supports mobility characteristics and the performance of the work done is not evaluated with the impact of the attack. The proposed work overcome the limitations of the key management mechanisms employed in the related work by evaluating the performance of the attack with increased number of malicious nodes in the network. The evaluation shows the improved network performance by lowering the energy, computational cost, and rate of packet loss.

3. Proposed work

3.1. Network model

The network model is shown in Fig. 1 which comprises of CH (Cluster Head), Sensor nodes and BS (Base Station) in the wireless sensor network which is divided into many forms of cluster based on the transmission range of the nodes. The cluster based network is used for the improvement of scalability and energy efficiency. The nodes are deployed in a geographical area to infer and measure the surrounding through its sensing capability and share the data in the environment. When the members in the cluster move to the different region then key management is an important concern in the cluster based wireless sensor networks. Also, the mobility of sensor nodes makes the network to random topology changes which lead to more security risks in the wireless sensor network. Our proposed scheme makes use of pre-distribution of random key and the algorithm selected here is multi hop distance based algorithm which enhances the energy efficiency and reduces the packet loss rate [8–12,21,23].

3.2. Key establishment and distribution

This phase is considered as phase-1 which is used for the generation of keys for every node in a cluster. All the nodes are pre-distributed with initial key K_i. After establishing the initial key, the master key K_m is generated using K_i and one way hash function f (h_x). The node SN_i will request a pairwise key from the node SN_j using its master key K_m. Then the message will be broadcasted to all the nodes in the network. After receiving the request, the node SN_j will send the pairwise key K_{pair} to the requested node SN_i. In this way, the pairwise key is established with single hop and multi hop nodes in the network. The key generation is based on a hash chain. The length of the hash chain fixed here is based on the compromised probability value. One way hash function is implemented for generating hash chain h_c. The domain key value K1 can be expanded to i times after h_c is applied on Ki. Now each cluster will hold at least one key among n keys generated by the hash function.

Table 1
Performance analysis of related work mechanisms.

Reference	Proposed schemes	Established links between nodes	Merits	Demerits
Lin You et al. [2]	One way hash chain based key with DKH-KD mechanism	One-hop	Improved performance in establishing a pairwise key.	Increase computational overhead because of the rekeying process
Danyang Qin et al. [3]	AKMS- pairwise key	One-hop	Enhance security by decreasing the computational cost.	The symmetric key is used
Ehdai et al. [4]	2D Hash-based key management	One-hop	More efficient against node capture attack.	Increase computational overhead.
Ahlawat et al. [5]	Pre distribution key	One-hop	It lowers the energy and computational overhead.	Pre distribution of key-based scheme
Priyanka et al. [6]	Hash chain based secure key management	One-hop	Resilience to node capture attack.	Increase computational cost.
Anita et al. [7]	Hybrid key-based key management	One-hop	Guaranteed security against malicious nodes.	Difficult to implement in practical scenarios.

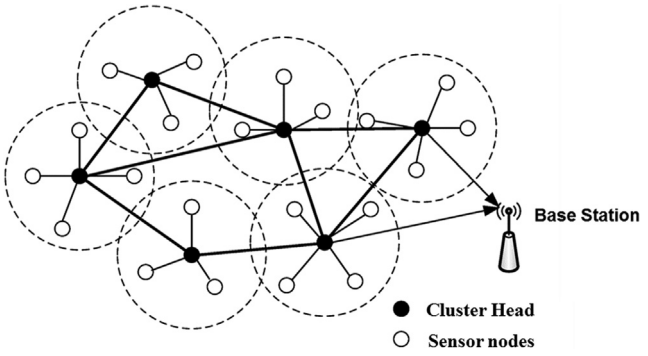

Fig. 1. System Model.

The information about each node in the cluster will be carried by every cluster CHi.

// ALGORITHM: MASTER KEY ESTABLISHMENT

// Initial key K_i is pre-distributed to all the nodes SNi..n

// Master key K_m is generated through K_i and f (h_x) during the initial stage

// Input: (SNIDi, $Nonce_i$): key generation request

// Result: Mater key K_m

VARs: CNi: Cluster Node; CHi: Cluster Head; Kpair pairwise key; K_i : initial key; K_m: Master Key; SN_i : Sensor Node; SNID : Sensor Node ID; f (h_x) : hash function;

1. Start
2. SNi sends the message (SNIDi, $Nonce_i$) to CH_i.
3. CHi authenticates SNi and validates the message (SNIDi, $Nonce_i$)
4. SN_i wait for the reply message for a random amount of time.
5. CH_i generates Master key K_m = f (K_i ($SNID_i$) and send it to $SNID_i$
6. Stop

3.3. Establishment of the pairwise key

After generating the master key K_m, the node A has to obtain its pairwise key to communicate with the destination node B. Assume that node A wants to communicate node B secretly by establishing pairwise key K_{pair}. Here each node in the cluster will have a pairwise key obtained from the established hash chain h_c. The establishment of a pairwise key is given as follows

For node A → h_{xa} ($h_{ya}(k_i)$)

For node B → h_{xb} ($h_{yb}(k_i)$)

The pairwise key for node A is generated as follows :

$$h_{xb}(h_{yb}(k_i)) \text{iff } X_a < X_b \text{ and } Y_a <= Y_b \quad (1)$$

For node B, pairwise key is generated $ash_{xa}(h_{ya}(k_i))$ iff $X_a > = X_b$ and $Y_a >= Y_b$ (2)

Therefore two nodes can generate a pairwiseright key $ash_{max}(h_{xa}(h_{ya}(k_i)))$ (3)

3.4. Key management process

Phase-1 generates master key Km and activates before the sensors are established in the network. Phase-2 describes the key predistribution which enables the security of the network. Phase- 3 is used for creating a secured link in multi hop distance. The First phase is the key distribution phase, here initial key Ki is generated and pre distributed with each node in the network during the deployment of the network. Each node SNi then will generate master key Km with Ki and one-way hash function Kh.

Sensor node n generates master key as

$$Km = f(K_i(SNID_i)) \quad (4)$$

After establishment of the master key in the initial phase, SNi will pass the node's identity information through the advertisement message to its neighbour node SNn and wait for the reply. Then neighbour node SNn receives the information and replies with its own identity information to SNi. Then both SNi and SNn generate pairwise key Km,n using their master key Km and Kn. After generating the pairwise with one hop distance neighbour nodes the nodes will also generate the pairwise key with multi hop distance neighbour nodes. If the source node is SNi and the destination node is SNn in multi hop distance then the pairwise key is calculated as

$$K_{i,j}, k...n = fK_iK_j, Kk...K_{n-1}(ID_n)$$

3.5. Authentication procedure for one hop neighbours

Fig. 2 shows the nodes in single hop distance. Mutual authentication will be performed when a new node need to connect in the network. If node A need to join in the network it sends Auth-Req to BS. The BS in turn reply with Auth-Res message encrypted with node A's public key and activate ACK1 in response to node A by validating node A's identity. While validating the request the BS will determine the encryption algorithm, protocols and public key of the requested node. Once authenticated, the node will have to periodically broadcast the "Hello" message to confirm its presence. If the BS does not receive any information from a particular node for some duration, then that node will be removed from the network.

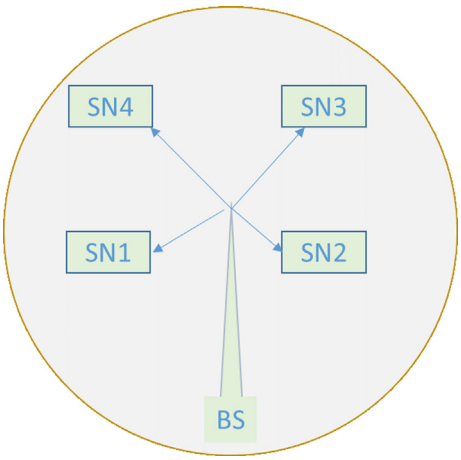

Fig. 2. Single hop nodes.

3.6. Authentication procedure for multi hop neighbours

Fig. 3 shows the nodes in multi hop distance. Mutual authentication will be performed upon request if a node in multi hop distance who is not in transmission limit wishes to connect in the network environment. The node who wishes to join in the network must be authenticated itself with BS directly attached to an authentication server. If node B in multi hop need to be connected with node A, it will send Auth-Req to BS since Node A cannot authenticate itself on behalf of BS. After receiving the request, it verifies its authenticity and activates ACK2, determines the algorithm, protocols and encrypts the response message with node A's public key and sends Auth-Res message to node B.

3.7. Routing protocol involved

Energy aware routing strategy is involved in this work. The steps consider below are contributed in the process of selecting the best path from a source node to the sink node.

1. Search for the sink node in the cluster to fix the next hop.
2. If the sink node is available, then fix the next hop as a sink node.
3. Check every node in the cluster for the best path towards the destination node.
4. Select a node for next hop based on the distance and signaling strength.
5. The distance measurement is done during the initial phase through the request-reply packet when all the nodes are sharing their details to CH node.
6. The node with the least distance metrics and strong signal strength considered to be the next hop node to reach the destination node.

4. Performance evaluations

This section evaluates and analyzes the performance of the work done in terms of the packet loss rate, energy efficiency and the enhanced security rate with various kinds of attacks.

4.1. Simulation details

The performance of the proposed work is analyzed by Ns-2 and the parameter used are shown in Table 2. The number of nodes considered in the simulation is 100 and attacks are 5, 10, 15, 20 and 25. The simulation considers the jamming attack by varying the malicious nodes in the real time scenario. The performance of the proposed scheme is measured using our key management scheme in the multi hop and without key management solution in the single hop for analyzing the packet loss rate. The implementation of the jamming attack shows that the attacker nodes block the network by continuously transferring the unwanted packets into the network. The routing protocol used here is energy aware routing method for cluster based dynamic environment [17]. This type of routing method helpful in distributing the energy evenly

Table 2
Simulation parameters.

Parameters	Value
Area	100 X 100 m
Network Interface type	IEEE802.15.4
Number of nodes	100
BS position	(50,250)
Initial energy(j)	0.5
Sensing range(m)	30
Packet size(bits)	1024
MAC	IEEE802.15.4
Threshold distance (m)	87
Energy receive	40nJ
Energy transmit	40nJ
Routing protocol	Energy aware
Traffic	CBR

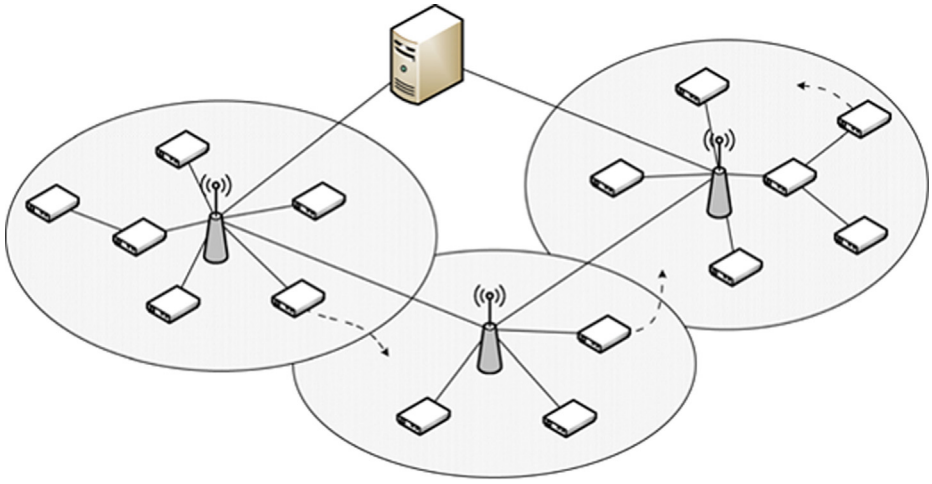

Fig. 3. Multi hop nodes.

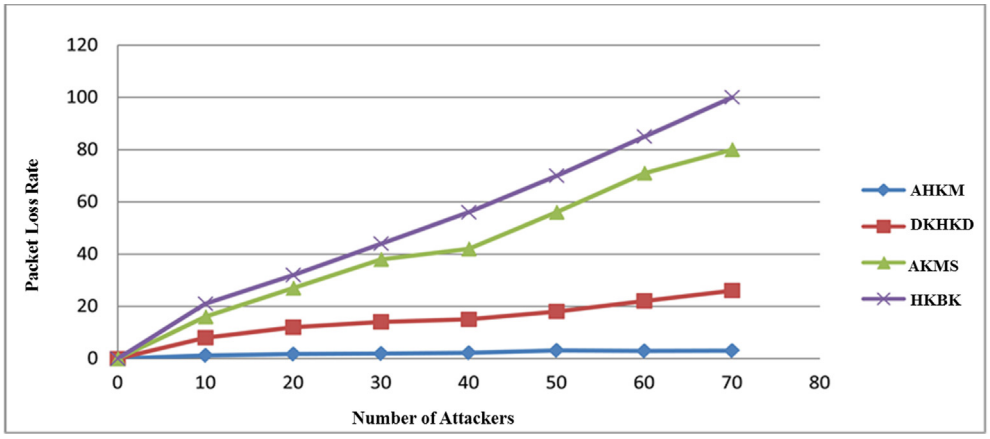

Fig. 4. Performance considering packet loss rate.

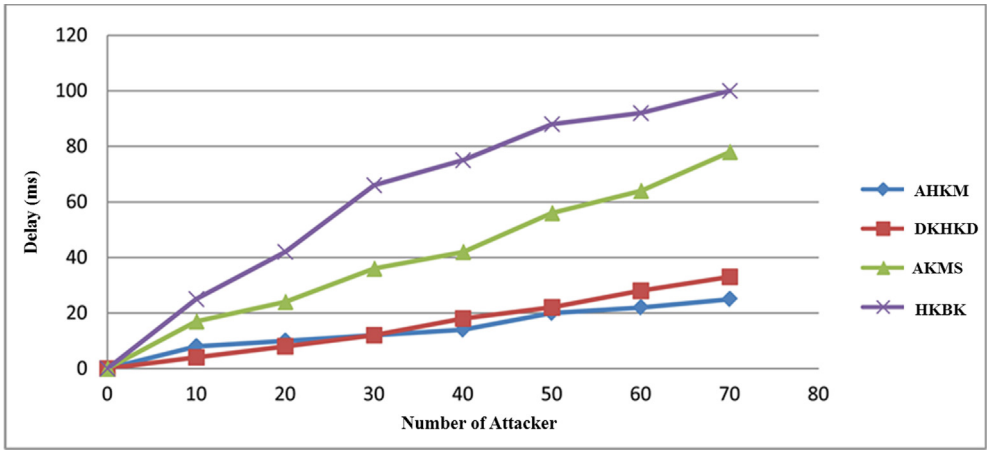

Fig. 5. Performance considering time delay.

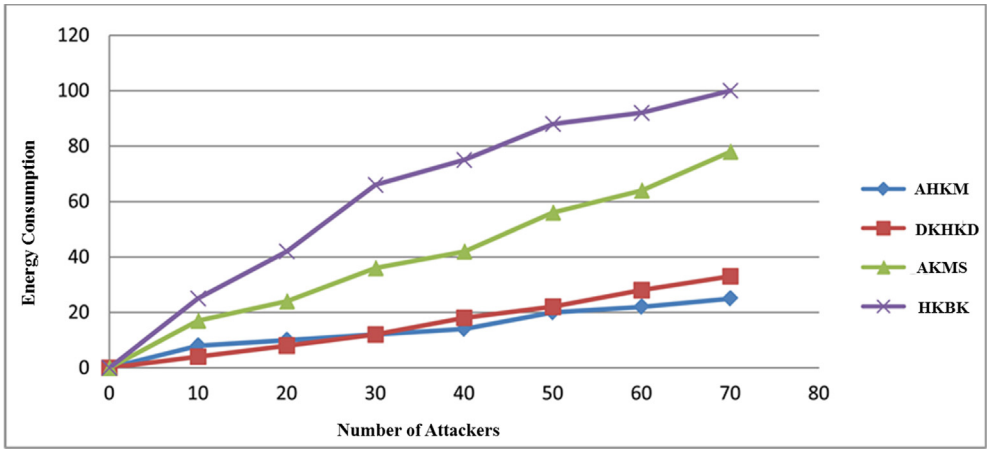

Fig. 6. Performance considering energy consumption.

to all the nodes connected in the network based on the minimum cost routing for the next hop.

4.2. Simulation results

Fig. 4, Fig. 5, and Fig. 6 show the performance of the network with one hop and multi hop solution considering energy consumption and time delay. The outcome of the simulation shows that the performance of the network is increased after implementing the proposed method with reduced packet loss, computational cost, energy and time delay. The performance degradation founded after a single hop key management scheme is applied. With a single hop scheme, the rate of packet loss increased during the attack, which leads to a huge number of retransmission of dropped packets. With the proposed combined solution, the improvement of packet loss rate and the energy consumption is obtained by having a single hop key for communicating with neighbour nodes and multi hop key for communicating with the multi hop node in terminus. The reason for the decreased computational overheads which are required for the key generation process is due to the one way hash

function used in the work [13,19,22]. One way hash function h_{ki+1}, $0 \leq i \leq n$ is calculated using pairwise key K_i to detect the malicious node. The malicious node in the network will be detected by CH through the key validation process. CH_i will maintain verifier V_n, $K_0 \leq n \leq K_n$ for every sensor node SNi in the network. In this process, each packet is investigated for its key and performs a verification process through the verifier function V_n. After verification, the packet will be dropped by CH_i if the function fails repeatedly for some fixed duration of time. After that, the malicious node will be removed from the network.

5. Conclusion and future work

The growth of wireless devices is increased day by day and the size of the network is expanding to a greater extent. This fast growth of smart devices needs strong security requirements to safeguard them from the security attacks. In this work, we proposed an improved hash based key management mechanism for multi hop networks. The importance of the hash function is to protect the stored password and to preserve the integrity of data. With the proposed hashing scheme, there is no need to encrypt the whole data using the secret key, but encrypting the hash value is sufficient. The entire communication path is verified to check whether the key management process is done properly using one way hash function. The attack can be mitigated and the malicious node will be removed from the network after investigating the arrival of each packet through the verification process done in the proposed work. The results show that the proposed work performed well in terms of packet loss rate, computational overheads, and energy efficiency. As a future extension, we plan to find a more efficient security solution to combat various versions of DDoS attacks on the wireless environment.

6. Funding/Financial support

The authors have no funding to report.

7. Other Support/Acknowledgement

The authors have no support to report.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Lin C, Wu G. Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach. J Supercomputing 2013;66(2):989–1007.
[2] Lin You, Younan Yuan, et al. A Key Distribution Scheme for WSN Based on Hash Chains and Deployment Knowledge. Int J Distrib Sens Netw 2015;11 (7):640792. doi: https://doi.org/10.1155/2015/640792.
[3] Danyang Qin, Shuang Jia, Songxiang Yang, et al. A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks. J Sens 2016;2016:1–9. doi: https://doi.org/10.1155/2016/1547963.
[4] Ehdaie M, Alexiou N, Ahmadian M, Aref MR, P.. Papadimitratos 2D hash chain robust random key distribution scheme. Inform Process Lett 2016;116 (5):367–72.
[5] Ahlawat P, Dave M. A hybrid approach for path vulnerability matrix on random key predistribution for wireless sensor networks. Wireless Pers Commun 2017;94(4):3327–53.
[6] Priyanka Ahlawat, Mayank Dave. An attack model based highly secure key management scheme for wireless sensor networks. ICSCC 2017:7–8.
[7] Mary Anita EA, Geetha R, et al. A Novel Hybrid Key Management Scheme for Establishing Secure Communication in Wireless Sensor Networks. wireless personal communications 2015;82(3):1419–33.
[8] Kahya N, Ghoualmi N, Lafourcade P. Key management protocol in WIMAX revisited. Adv Comput Sci Eng Appl 2012;167:853–62.
[9] Ciou Yi-Fu, Leu Fang-Yie, et al. A Handover Security Mechanism Employing the Diffie-Hellman Key Exchange Approach for the IEEE802.16e Wireless Networks. Mobile Inform Syst 2011;7(3):241–69. doi: https://doi.org/10.3233/MIS-2011-0120.
[10] He X, Neidermeier M, Meer H. Dynamic key management in wireless sensor network: a survey. J Network Comput Appl 2013;36:612–22.
[11] Wu G, Chen X, Obaidet MS, Lin C. A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set. Security Commun Networks 2012;6:230–8.
[12] Bechkit W, Challal Y, Bouadallah A. A new class of hash chain based key predistribution scheme for WSN. Comput Commun 2013;36:243–55.
[13] Ziyue Wang, Bing Zhao, Xiaobing Liang, and Yuemin Ding, Enhanced Key Management Protocols for Wireless Sensor Networks, Mobile Information Systems,vo.10 , No.1, January 2015.
[17] Feroz Khan AB, Anandharaj G. A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT". SN Appl Sci 2019;1(12):1575.
[19] Ali Inayat, Sabir Sonia, Ullah Zahid. Internet of things security, device authentication and access control: a review. Int J Comput Sci Inform Security (IJCSIS) 2019:1901.07309.
[21] Cooremans Catherine, Schönenberger Alain. Energy management: A key driver of energy-efficiency investment?. J Cleaner Prod 2019;230(1):264–75.
[22] Athmani Samir, Bilami Azeddine, Boubiche Djallel Eddine. EDAK: an efficient dynamic authentication and key management mechanism for heterogeneous WSNs. Future Generation Comput Systems 2019;92:789–99.
[23] Sandro Nižetić, Nedjib Djilali Agis Papadopoulos, Joel J.P.C.Rodrigues, Smart technologies for promotion of energy efficiency, utilization of sustainable resources and waste management, Journal of Cleaner Production, Volume 231, 10 September 2019, Pages 565-591.

Further Reading

[14] Samira Mesmoudi, Belkacem Benadda and Amin Mesmoudi. SKWN: Smart and dynamic key management scheme for wireless sensor networks, IJCS, April 2019.
[15] Sharma Ashish. Improved attribute based encryption scheme in cloud to representative authorization framework for EHR services. IJCA 2019; 12(6).
[16] Ahlawat P, Dave M, A Hybrid Approach for Path Vulnerability Matrix on Random Key Predistribution for Wireless Sensor Networks Wireless Personal Communications, 94 (4) (2017), pp. 3327-3353.
[18] Balasubramanian, Prabhu kavin, SannasiGanapathy, A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications, Computer Networks, Volume 151, 14 March 2019, Pages 181-190.
[20] Ghosal Amrita, Conti Mauro. Key management systems for smart grid advanced metering infrastructure: a survey. IEEE Commun Surv Tutorials 2019. doi: https://doi.org/10.1109/COMST.2019.2907650. Volume: 21, Issue: 3, March.

Feroz khan A.B is currently a PhD research scholar at the faculty of computer science, Adhiparasakthi College of arts and sciences, Kalavai, India. He is working as an Associate Professor at C.Abdul Hakeem College of Engineering and Technlogogy, Vellore, India. He received his M.C.A degree in Computer Science and Applications from Jamal Mohammed College, Bharathidasan University, Tiruchirapalli, India in 2005. He also received M.E degree in Computer Science and Engineering from C. Abdul Hakeem College of Engineering and Technology, Vellore, India in 2015. He has presented several papers at national and international levels and published research papers in leading journals. He is also a reviewer of several journals such as Wireless personal Computing, The Journal of supercomputing, International journal of communication system, Journal of computer security, Journal of Engineering Research, Journal of organizational and end user computing, and Journal of Intelligent and Fuzzy Systems. His research interests include wireless sensor networks, Cryptography and Network Security, and Internet of Things.

Dr. G. Anandharaj is currently working as Assistant Professor and Head in the Department of PG and Research Department of Computer Science,Adhiparasakthi College of Arts and Scince, Kalavai 632506. He has obtained his MCA Degree from Bharathiar University, M.Phil (Computer Science) in Bharathidasan University and Ph.D from Anna University. He has vast experience in teaching as well as research. He has presented papers at several International and National Conferences and has published research articles in leading Journals. His research interests include mobile computing and wireless network technology. He is life member of the ISTE. He has guided ten M.Phil students and currently guiding four Ph.D (Research) scholars in Thiruvalluvar University.