Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network using Hybrid Approach

Sharmila
Krishna Engineering College
Pramod Kumar
Krishna Engineering College
Shashi Bhushan
Krishna Engineering College
Manoj Kumar (wss.manojkumar@gmail.com)
University of Petroleum and Energy Studies https://orcid.org/0000-0001-5113-0639
Mamoun Alazab
Charles Darwin University

Research Article

Keywords: Wireless Sensor Networks, Security, Computing, Crypto-graphic, Authenticatio

Posted Date: March 19th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-328155/v1

Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network using Hybrid Approach

[1]Sharmila, [2]Pramod Kumar, [3]Shashi Bhushan, [4]Manoj Kumar, [5]Mamoun Alazab
[1]Department of Electronics and Communication Engineering, Krishna Engineering College, Uttar Pradesh, India
[2]Department of Computer Science Engineering, Krishna Engineering College, Uttar Pradesh, India
[3,4]School of Computer Science, University of Petroleum and Energy Studies, Dehradun
[5]IT and Environment, Charles Darwin University, 0909 Darwin, Australia

[1]sharmila1ece@gmail.com, [2]pramodkumar.hod@krishnacollege.ac.in,
[3]tyagi_shashi@yahoo.com, [4]wss.manojkumar@gmail.com, [5]alazab.m@ieee.org

Abstract: Wireless Sensor Networks (WSNs) play a crucial role in developing the Internet of Things (IoT) by collecting data from hostile environments like military and civil domains with limited resources. The above applications are prone to eavesdropper due to cryptographic algorithms' weaknesses for providing security in WSNs. The security protocols for WSNs are different from the traditional networks because of the limited resource of sensor nodes. Existing key management schemes require large key sizes to provide high-security levels, increasing the computational and communication cost for key establishment. This paper proposes a Hybrid Key Management Scheme for WSNs based on Elliptic Curve Cryptography (ECC) and a hash function to generate key pre-distribution keys. The Key establishment is carried out by merely broadcasting the node identity. The main reason for incorporating a hybrid approach in the key pre-distribution method is to achieve mutual authentication between the sensor nodes during the establishment phase. The proposed method reduces computational complexity with greater security and the proposed scheme can be competently applied into resource constraint sensor nodes.

Keywords: Wireless Sensor Networks, Security, Computing, Cryptographic, Authentication

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have been used in numerous fields like monitoring hostile environments, armed and civil domains in a short span of time. The sensor nodes placed in an unfriendly location are prone to the node compromise attack [1-5]. As the sensor node communicates wirelessly, it is easy for an attacker to compromise the nodes' communication. To overcome the attacks of the WSNs, security must be integrated with the network. Providing security in WSNs is thought-provoking due to sensor nodes' resource constraint nature, but secure communication can play a significant role in avoiding different attacks. The security in WSN can be achieved with encryption and

authenticating the communication among the sensor nodes. The limitations mentioned above can be avoided with the aid of a key management scheme.

A key management scheme can be widely utilized to secure communication between the sensor nodes within its range. The key management scheme is divided into 3 phases- key pre-distribution, shared key discovery, and key establishment [6-10]. Initially, the keys are pre-distributed into the sensor nodes (i.e., before node deployment). Once nodes are placed in the field, each node tries to determine a shared key within its communication range. During the second phase, the neighboring sensor nodes form a shared key for secure communications.

In recent times, numerous key management schemes have been suggested to establish secure communication among the sensor nodes during the network formation. Each of these schemes has its advantages and limitations. The suitable key management scheme should satisfy three important metrics [11-13]: security, efficiency, and flexibility.

The limitations of the existing key pre-distribution schemes depend on symmetric and asymmetric cryptographic techniques are as follows:

•The major limitation of Elliptic Curve Cryptography (ECC) based key pre-distribution schemes is that the keys are generated directly using ECC and pre-distributed into the sensor node. This increases communication costs and the requirement of memory. The key establishment between the sensor nodes are not addressed in the existing ECC-based key pre-distribution scheme.

•The Random Seed Distribution with Transitory Master Key scheme (RSDTM) [20-22] is the Random Seed Distribution's major limitation because a node cannot establish a shared key after a certain time. If an adversary captures anode's master key, then the entire network can be compromised by an attacker.

• In E-G scheme [18], the sensor nodes need to store a vast number of keys to increase sensor networks' connectivity. However, it provides neither authentication nor key revoking between sensor nodes. Moreover, the scheme requires more memory for key storage.

This paper's main contribution is to overcome the above limitations; the proposed key management Scheme for WSNs reduces memory requirement, computational and communication overhead. It integrates both the cryptography techniques to achieve a high level of security and improves a node-to-node authentication compared to the existing key management scheme such as E-G and RSDTM.

The structure of the paper is arranged as follows: Section 2 reviews the related works of existing security schemes for WSNs. Section 3 explains the proposed scheme by integrating the authentication and secure key establishment using a hybrid approach. Section 4 describes the theoretical investigation of the proposed scheme. Section 5 reviews the simulation result and analysis of the proposed method. Section 6 summarizes the proposed method.

2. RELATED WORKS

Eschenauer et al. [18] proposed the key management scheme based on the probabilistic method for WSNs. E-G scheme is depending on a random graph structure. This scheme is specially offered for wireless sensor networks. Most of the research work for WSNs is a framework of E-G methods. The major limitation of E-G scheme is no authentication, poor connectivity and periodic key refreshing is not done. The key should be refreshed peri-

odically in order to overcome node compromised attacks. It does not support clustering operations to minimize the consumption of energy. Chan et al. [17] proposed the Q-composite and multipath key reinforcement scheme. The Q-composite method is the extension of EG-Scheme. The sensor nodes' network resilience is improved by using more keys instead of a single key in the EG scheme. The main advantage of this scheme is improved the resilience of network against node compromise attack. However, this scheme is more susceptible to attack once more numbers of nodes are compromised.

The pairwise key is generated by Blom's scheme [19]. The pairwise key is established among neighboring nodes in the network. It uses the threshold property to attain high resilience. The attacker needs to capture more nodes (i.e., greater than the threshold value) to capture the whole network. When the threshold value increases, the storage space required to hoard the keys also increases. To secure the WSNs, several key management schemes have been suggested [2-19].

The symmetric pre-distribution scheme offers security efficiently but not appropriate for the unfriendly environment. Gandino et al. [20-23] proposed a Random Seed Distribution with Transitory Master Key scheme (RSDTMK), in which the seed keys are stored inside the sensor nodes instead of plain keys. In the initialization phase, the node generates the pairwise key using the master key within the activated time period. The main limitation of this scheme is the key cannot be generated after the time-out period. If the attacker compromised the master key, eavesdrop on the entire key information within the initialization phase and discovers the entire pairwise key shared between the nodes.

Public key cryptography plays an important role in cryptographic techniques. It has a private and public key. The key size of public-key cryptography needs to be high to offer a high level of security. The direct implementation of public-key techniques is not suitable for resource constraint sensor nodes.

Many research works have been carried out on resource constraint network using public-key cryptography. Asymmetric key cryptography techniques need to perform more computation for encryption and decryption operation. It needs more computational power and processing time for performing the operation. Rivest Shamir Adleman (RSA) algorithm proposed RSA algorithm in 1977 [24]. It uses 512 to 2048 bits as key size. Many research works have been carried on Elliptic Curve Cryptography using 8-bit CPUs. As compared to RSA, the key size of ECC is small. TinyOS key pre-distribution method is depends on ECC. For the RSA algorithm, the key size is 1024 bits, whereas for ECC, the key size is 160 bits for secure communication.

The elliptic curve cryptography based key pre-distribution scheme [29] is proposed for WSNs. The keys are generated by performing a point doubling operation. It offers high connectivity as well as resilience for the resource constraint nature of sensor nodes. This scheme's limitation is the plain keys (ECC points) are pre-distributed into the sensor node. The author did not address the issue of how the sensor nodes have established the key among the sensor nodes, and communication overhead is high. Du et al. [32] demonstrated routing-driven key management scheme using elliptic curve cryptography for WSN. This scheme's performance is carried out in heterogeneous sensor networks to achieve high-level security in WSNs. It establishes shared keys with neighbor nodes using ECC based digital signature.

One of the evolving techniques of cryptography is Hyper Elliptic Curve Cryptography (HECC). The security level of HECC is the same as RSA and ECC and the key size is 80 bits [33-35], whereas 1024 bit for RSA and 60 bits for ECC.

The approaches above for WSNs emphasize the distribution of key between the sensor nodes and not on node-to-node authentication. Thus, in this paper, the hybrid key management scheme method is proposed to provide authentication between nodes and reduce storage space, computational and communication overhead.

3 PROPOSED KEY MANAGEMENT ALGORITHM FOR WSNs

In the proposed hybrid key management scheme, key pre-distribution depends on ECC and a hash function. Before deploying sensor nodes, three offline and one online phase are performed, namely parameter selection for the elliptic curve, generation of unique seed key, identity-based key ring generation, key establishment, and mutual authentication phase. A unique seed key is generated from the elliptic curve equation, which is preloaded to each sensor node, and a hash function is used on the seed key to generate the private key. Then, the generated key-ring and their corresponding identities are loaded into the sensor nodes memory. Once nodes are placed in the field, sensor nodes disseminate their ID to form common keys with other nodes. The nodes are mutually authenticated using their own identity of nodes without a huge communication overhead.

3.1 Parameter Selection for Elliptic Curve

Before sensor nodes deployment, the server generates the key pool using the Elliptic Curve Cryptography equation over an integer finite field. The elliptic curve parameters selection is vital in wireless sensor networks to reduce the number of links compromised by an attacker and improve network connectivity. The elliptic curve parameters $p,$ a, and b are chosen where the value of prime number p should be greater than the total nodes deployed in the field. For example, if the number of nodes deployed in an area is 50, the prime number's value should be greater than 50 to improve the connectivity at the same time to increase the resilience.

3.2 Generation of Unique Keys

Unique keys are generated before sensor nodes are deployed in the area. Once the ECC equation's coefficients are chosen, the unique seed keys are produced for sensor nodes.

3.3 Identity based Key Ring Generation

In this proposed scheme, the key-ring selection depends on the node's ID, unique seed key, and hash function. The identity-based key-ring selection has more advantages compared to the pseudo-random sequence [20]. During the key establishment phase, the node has to interchange its identity for peer nodes to obtain the shared key. This also provides legitimacy of the entity. In the pre-deployment phase, the server assigns a unique identifier ID_i , hash function h_j, and seed key $[u, v]$ to each sensor node.

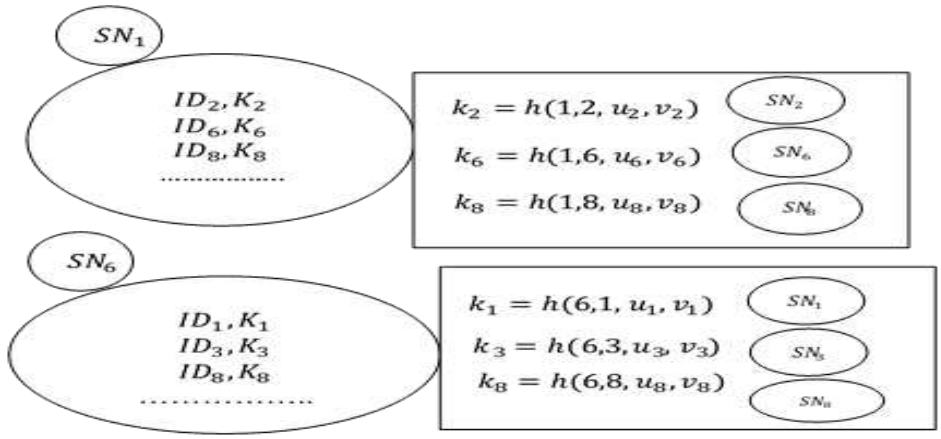

Fig.1 Key Predistribution of Hybrid Key Management Scheme.

The server randomly chooses ' m' other sensor nodes to generate the unique key-ring using a simple hash function and store the keys and their corresponding identities into the sensor node memory. The following equation generates the key Ki,

$$K_i = h_j(u_i, v_i) \quad (1)$$

Consider an example as presented in Fig.1, the sensor mote S_1 randomly selects three sensor nodes S_2, S_6 and S_8 from the network and generates the key-ring K_2, K_6 and K_8 using a hash function on their corresponding seed key and load the key indices and ID of the sensor nodes in key-pool. Similarly, it stores $'m'$ pairs of key and ID in the key-ring, where m is the key-ring size.

3.4 Key Establishment and Mutual Authentication Phase

Once the keys are distributed, the sensor nodes are randomly disseminated in the field. In the initialization step, each sensor node shares its ID_i and receives neighborhood nodes' ID.

Consider the nodes ID_j, which is in the range of sensor mote ID_i, verifying that the received ID_i belongs to the key-ring stored in the sensor node before the deployment. If it is in their key-ring, it chooses a timestamp to avoid replay attack and shares the joint request message to the corresponding node ID_i. Once the sensor node ID_i receives the joint request message, it computes C' and verifies that $C = C'$. If $C = C'$, the node is mutually authenticated and generated the session key by computing $S_k = K_i + K_j$. There are two cases in the key establishment phase, namely the direct and indirect key establishment phase. The algorithm is explained as follows,

Algorithm:
$Input: ID\ of\ receiver\ sensor\ node\ ID_i$
$Output:\ Session\ key\ K_{ij}$
$Step: 1 \quad i \rightarrow *: < ID_i, T_1 >$
$Step: 2\ j = discover(ID_i \in m)$
$if\ (ID_i \in m)$
$C = h(K_1, ID_1)$
$j \rightarrow i: < ID_j, T_6, C >$
$Step: 3 \quad if\ (ID_i \in m)$
$C_1' = h(K_1, ID_1)$
$S_k = K_i \oplus K_j$

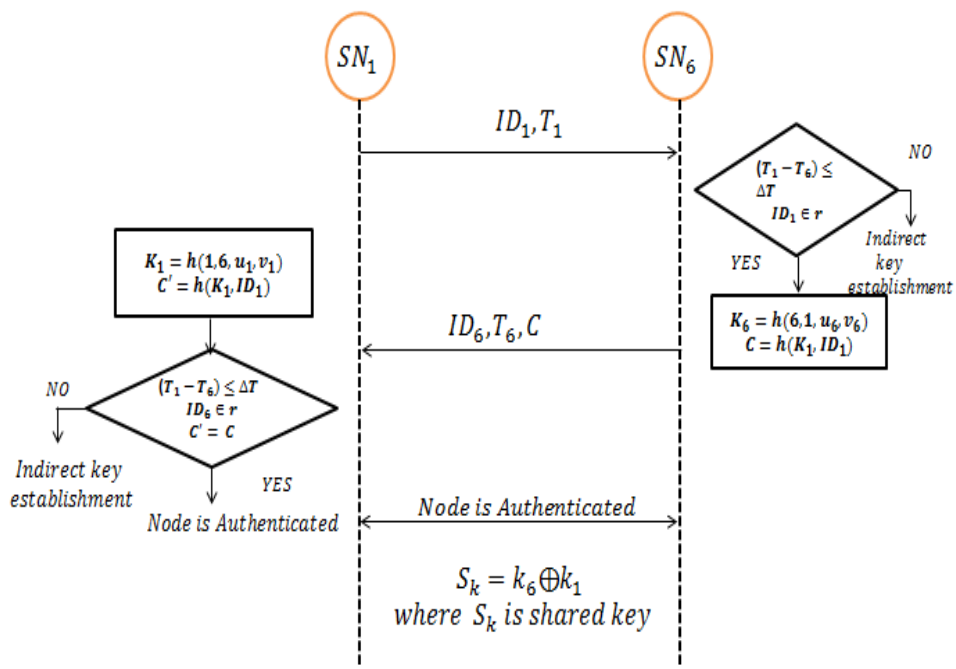

Fig.2 Direct Key Establishment between the Nodes

Case: 1 Direct key establishment between the nodes

After sensor nodes are disseminated in the area, it broadcasts the unique ID and timestamp to the neighboring nodes within the broadcasting range. The sensor node which receives the neighbor information validates the timestamp to avoid the replay attack and checks the received identity as to whether it belongs to the key-ring or not. If the sensor node's identities belong to the key-ring, then it transmits $C = h(k_1, ID_1)$ where $k_1 = h(1,6,u_1,v_1)$ and timestamp to node 1.

Node 1 receives the authentication message from node 6; it checks the timestamp and verifies its key-ring. If ID_6 belongs to the key-ring, SN_1 calculates the $C' = h(k_1, ID_1)$ and verifies if $C = C'$, then it authenticates node 6 and computes the session key $S_k = K_1 \oplus K_6$. Fig.2 shows the direct establishment of keys among the sensor nodes.

Case: 2 Indirect key establishments between the nodes

If the identity of the SN_1 does not belong to the key-ring, then the sensor node 6 computes D where $D = h(K_6, ID_1)$ and shares it to the sensor node 1. The sensor node 1 verifies the identity of sensor node 6, and if it belongs to the key-ring, it verifies $D' = D$ and authenticates node 6. Node 1 computes $'m'$, where $m = E_{K_6}(K_1)$ and transmits the value of $'m'$ and its identity to node 6. Node 6 decrypts the message with the help of K_6 and obtains the K_1. Then the session key is formed by $S_k = K_1 \oplus K_6$. Fig.3 shows the operation of indirect key establishment between the sensor nodes.

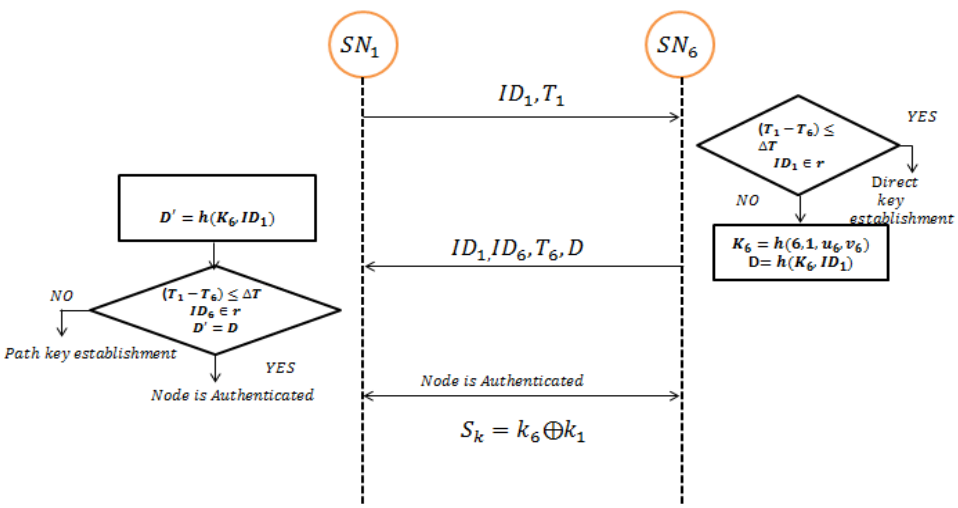

Fig.3 Indirect Key Establishment between the Nodes

3.5 Path Key Establishment

If the common key is not shared among the two nodes, it tries to establish a path key through an intermediate node using the same handshake protocol.

4. PERFORMANCE ANALYSIS OF THE PROPOSED HYBRID APPROACH

The proposed system's effectiveness has been analyzed theoretically with the help of storage requirements and communication costs. The proposed scheme's performance is analyzed with the help of the parameters such as the number of nodes in the network, keys in the key pool, and hop count.

4.1 Memory Storage Requirement Analysis

The storage requirement has been analyzed to evaluate the efficiency of the protocol. The metrics that describe the efficiency of storage are key ring size (r), length of the seed key (l_s), key identifier (l_{kID}), length of the key ($_{UK}$), and the number of neighbors (v).

Table 1. Memory storage space required for shared key

Scheme	E-G	RSDTMK	ECC	HKMS
Initial Storage	$r.(l_k + l_{kID})$	$r . l_s + l_k + r.l_{sID} + l_s + l_p$	$r(K_i + l_{ID})$	$r(K_i + l_{ID})$
Working Phase	$r.(l_k + l_{kID}) + v.$ $(l_{ID} + l_{kID})$	$r.(l_k . l_{kID}) + v.$ $(l_{ID} + l_{kID})$	$r .(K_i + l_{ID_k}) + v.$ $(l_{ID} + l_{kID})$	$r(K_i + l_{ID})$ $+ v((K_{i,j})$

Table 1 shows the storage space required to store the key material in sensor nodes. The following metrics can assess the memory capacity required for the proposed scheme, namely the key-size($_{UK}$) as 160 bits long, node ID 2 bytes, key-ring size of 10, the memory required to store the key information for the HKMS is 202 bytes, whereas in E-G scheme it is 220 bytes [18] and for the RSDTMK 316 bytes [22]. The proposed scheme's storage capacity is 18 bytes less compared to the E-G and 114 bytes compared to the RSDTMK scheme.

4.2 Communication Efficiency

In this proposed scheme, finding the key among two nodes requires one-hop communication between nodes as in E-G and RSDTMK; but the message's size is different for each scheme. In HKMS, once nodes are disseminated in the field, it initiates the communication by sending a hello message containing the node and timestamp's identifiers. The acknowledged message contains the node's identifier, neighbor node identifier, and Message Authentication Code (MAC) of the message (c).

Table 2. Communication efficiency

Scheme	Hops	Number of Messages	Size of Transmitted Data
$\mathrm{E-G}$	1	2	$(r+1).l_{KID} + 2.l_{ID} + l_k$
RSDTMK	1	2	$r.l_{SID} + l_{KID} + 2.l_{ID} + l_k$

HKMS	1	2	$3.l_{ID} + v.l_{KID} + T_s$

Table 2. shows the comparison of communication efficiency of EG, RSDTMK and HKMS. Considering the $l_k(MAC) = 16\ byte$, $l_{ID} = 2\ byte$, $l_{SID} = 2\ byte$, $r = 10$ and in E-G $l_{kID} = 2\ byte$ and RSDTMK $l_{kID} = 3\ byte$, RSDTMK needs 43 bytes to establish a pairwise key, whereas in E-G scheme, 42 bytes and HKMS requires only 26 bytes to establish a secure key establishment. From this theoretical analysis, it is inferred that the proposed HKMS requires a smaller number of bytes to form a secure communication between the sensor nodes.

5. SIMULATION RESULTS AND DISCUSSION

To assess the performance of the HKMS protocol, the NS 2.35 simulator has been used. The analysis is emphasized on the formation of the keys in the network.

Table 3. Simulation Parameters and its Value

Parameters	**Values**
Sensing Area	1000m X 1000m
Number of Nodes	100
Simulation Time	20 secs
Initial Energy	50 Joules
Radio Propagation Model	Two Ray Ground model
MAC	IEEE 802.11
Antenna type	Omni antenna
Broadcast Interval	10ms

Generally, the key establishment schemes are focused only on the generation and establishment of keys which does not provide mutual authentication and key exchange among the sensor nodes. The proposed key management's performance is analyzed in terms of resilience, connectivity/channel existence of the network, network availability, broadcast delay, and energy consumption. The simulation parameters used to assess HKMS, E-G and RSDTMK are given in Table 3.

5.1 Connectivity Analysis for HKMS with E-G and RSDTMK

The connectivity is the establishment of a communication channel among two sensor nodes when they share a minimum of one key. The probability of secure link establishment among the two nodes [18] can be defined by,

$$P(i,j) = (((K_s - m)/m)/(K_s/m)) \quad (2)$$

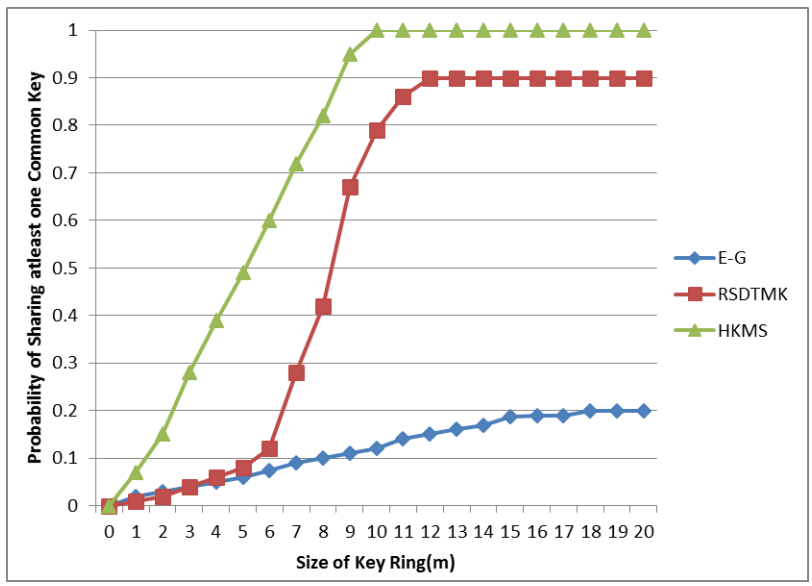

Fig. 4. Connectivity Analysis of HKMS with E-G and RSDTMK

The probability of link established between the sensor nodes in the network depends on the value of K_s and m; where K_s is key size and m is key-ring size. The value of m is the same for all the sensor nodes. Fig.4. shows that the probability of the link exists between the nodes disseminated in the network. From the resulting output, it is inferred that 100% of connectivity is achieved by the proposed scheme for the key-ring size of 10 whereas in E-G and RSDTMK were 10% and 80%, respectively for key-ring size of 10. The simulated results indicate that the proposed HKMS scheme increases 80% and 10% of connectivity compared with E-G and RSDTMK.

5.2 Comparison of Resilience for HKMS with E-G and RSDTMK

The resilience is defined as the ability to reduce the compromising of secret key materials loaded in the sensor nodes. Assuming that the link between sensor i and j is under the attack, the attacker compromises the link form a union $A = \{a_1, \ldots a_n\}$ of $a > 0$ means compromised sensor nodes.

The probability of key sharing among the node i and j is not present in the set A [22] is given by,

$$\overline{\Pr}(S_{i,j}) = \Pr\left[\left(m^1{}_i \in m_j \ \wedge \ m^1{}_i \notin A\right) \vee \ldots\ldots\ldots \left(m^k{}_i \in m_j \ \wedge \ m^k{}_i \notin A\right)\right] \quad (3)$$

The probability of the coalition of k trials can be given by,

$$\Pr(S_{i,j}) = 1 - \sum_{s=1}^{k}(-1)^{s+1}\binom{k}{s}\left(\binom{p-s}{k-s}/\binom{p}{m}\right)\left(\binom{p-s}{k-s}/\binom{p}{m}\right)^{a} \quad (4)$$

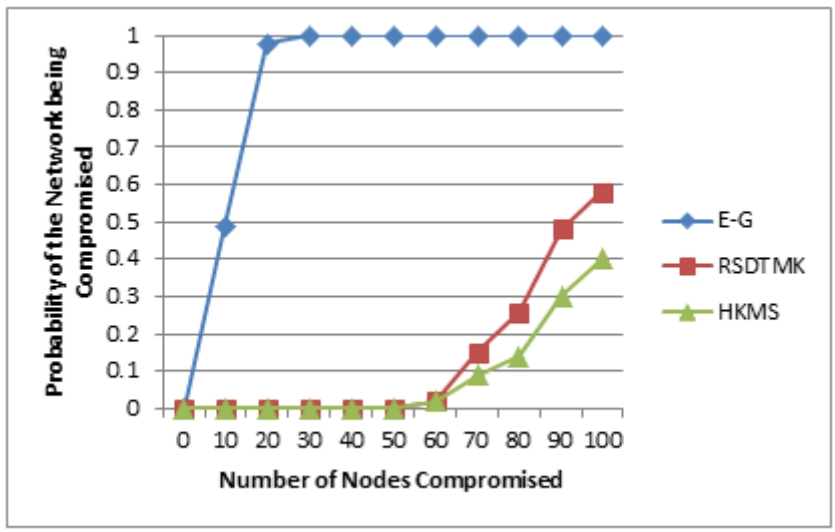

Fig. 5. Connectivity Analysis of HKMS with E-G and RSDTMK

Fig.5 shows the probability of compromising a linkage between the sensor nodes by an attacker for different values of p, a and m and the network secured by the proposed method compared to the basic E-G and RSDTMK schemes. The simulation results show that the proposed scheme decreases the probability of links compromised between sensor nodes by 39% compared to the existing schemes.

In the E-G scheme, the attacker compromised 50% of a communication link in the network by capturing 10 sensor nodes that are minimal resistant to node capture attack. When the invader/attacker captures 50 to 60 nodes, the whole network is thoroughly compromised. In the proposed approach, the invader requires capturing more sensor nodes to compromise the link between the nodes. It provides more resistance against node capture attack even though the attacker knows the key-ring compromised node's key-ring. The key pool reconstruction is not possible because the key-rings are generated by one way hash function. In the initialization phase, the sensor node broadcasts its identity instead of sharing the seed key stored in the key-ring. The proposed HKMS abides against the node capture attack and provides mutual authentication between the sensor nodes.

5.3 Analysis of Energy Consumption for HKMS with E-G and RSDTMK

Energy consumption is referred to as the total quantities of energy drained by the nodes in the wireless sensor network to establish a common key by performing computation and broadcasting the key information related to the key establishment.

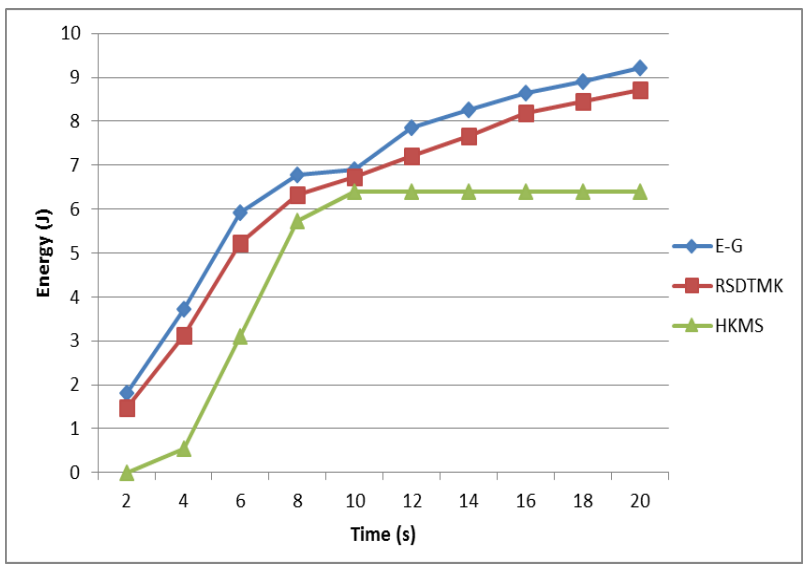

Fig. 6. Comparison of Transmission Energy Consumption of HKMS with Existing Schemes

The decisive factor of communication consumption is the message's size being transmitted or broadcasted to form a key between sensor nodes. The energy consumed by each protocol to establish a shared key is shown in Fig.6.

The simulated results concluded that energy consumption for HKMS conserves 30.67% of transmission energy compared to the existing E-G and RSDTMK scheme.

5.4 Comparison of Packet Broadcast Delay for HKMS with Existing Schemes

The broadcast delay is an important problem for critical event monitoring in WSNs. Fig.7 shows the broadcast delay of the sensor nodes in the network. The proposed protocol broadcast delay is 13.07% lesser than the existing scheme. It requires minimum time delay to establish a key between the neighbor nodes. Each node requires only to broadcast its identity during the key establishment phase. The proposed protocol reduces the time delay and the number of packets needed to communicate with neighboring sensor nodes for establishing a session key.

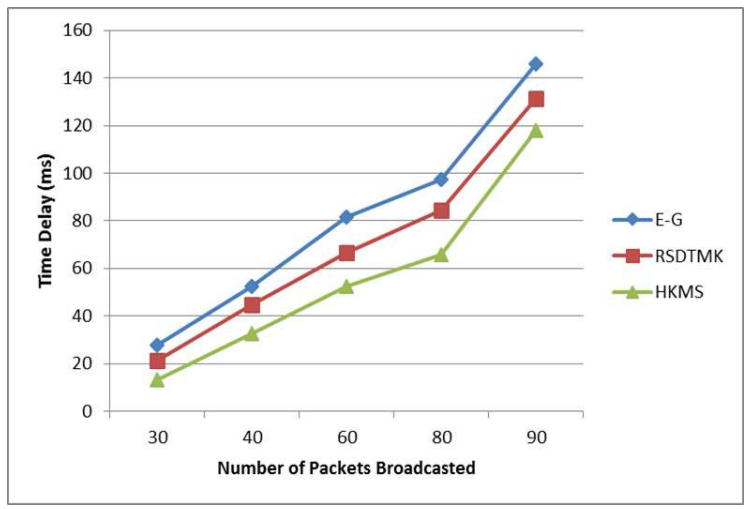

Fig. 7. Packet Broadcast Delay Analysis of HKMS with E-G and RSDTMK

The proposed HKM scheme is compared with the E-G scheme [18] and RSDTMK Scheme [20] for the above-discussed metrics. The performance values are tabulated in Table 4. From Table 4, it is inferred that the performance of HKMS is better when compared to E-G and RSDTMK.

Table 4. Comparison of Different Techniques with respect to various parameters

Parameters	**E-G**	**RSDTMK**	**HKMS**
Connectivity for Key Ring Size (r=10)	12%	80%	100%
Resilience with respect to Number of Node Compromised (70)	100%	15%	9%
Energy Consumption	9.2J	8.8J	6.2J
Packet Broadcast Delay	145ms	128ms	118ms

6. CONCLUSIONS

A hybrid key management scheme for WSNs to pre-distribute and establish the secure and authenticated communication link between the nodes using symmetric and asymmetric key cryptography have been proposed. The hybrid scheme incorporates the advantages of ECC based key pre-distribution scheme with a hash function and shared key between the nodes, which can be achieved by broadcasting the node's identity without sharing the key materials. The proposed Hybrid Key Management scheme conserves 30.67% of transmission energy and broadcast delay is 13.07% lesser than the existing scheme. The HKMS increases the connectivity and the probability of link compromise between the sensor nodes decreased by 39% than the existing methods. The performance

study of the proposed key management scheme shows that the link formation between the nodes increases, provides mutual authentication among the nodes, and resists against node capture attack compared to the basic E-G and RSDTMK scheme. However, to effectively increase the lifetime of WSNs with less energy consumption, the WSNs necessitates the Energy-efficient hierarchical routing protocol

REFERENCES

1. I.F.Akyildiz, W.Su, Y.Sankarasubramanium, and E.Cayirci, “Wireless sensor networks: a survey,” *Elsevier Computer Networks*, vol.38, pp.393-422, 2002.
2. R. Sharmila, and V.Vijaylakshmi, "Hybrid Key Management Scheme for Heterogeneous WSN's", *International Journal of Knowledge Engineering and Soft Data Paradigms (IJKESDP),*Inderscience Publications,vol. 6,no. 2, pp.95-109, 2019.
3. R.Sharmila, V.Vijayalakshmi, and R.Rajashree, “An energy-efficient routing protocol using hybrid evolutionary algorithm in wireless sensor networks”, *International Journal of Knowledge Engineering and Soft Data Paradigms*, vol. 5, no. 3/4, pp.285–301, 2016.
4. E.Yuan, L.Wang, S.Cheng, N. Ao, and Q. Guo. “A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks, *Sensors*. 20, issue.1543, 2020.
5. Qik Zhang, Yongjiao Li, Quanxin Zhang, and Junling Yuan. “A self-certified cross-cluster asymmetric group key agreement for WSNs, *Chinese Journal of Electronics*, vol. 28(2), pp: 280-287, 2019.
6. D.Kandris, C.Nakas, D.Vomvas, and G.Koulouras, “Applications of Wireless Sensor Networks: An Up-to-Date Survey”. *Application. System. Innovation,* vol.3, no.14, 2020.
7. Al-taha, and A.Mohammed, “Symmetric Key Management Scheme for Hierarchical Wireless Sensor Networks”, *International Journal of Network Security & Its Applications (IJNSA)*, vol.10,no.3, May 2018.
   Available at SSRN: https://ssrn.com/abstract=369622510.3390/asi3010014.
8. K. Hamsha and G. S. Nagaraja, "Threshold cryptography-based lightweight key management technique for hierarchical WSNs,” Ubiquitous *Communications and Network Computing*, vol. 276,pp. 188–197, May 2019.
9. A. Kumar, N. Bansal, and A. R. Pais, “New key pre-distribution scheme based on combinatorial design for wireless sensor networks,” *IET Communications*, vol. 13, no. 7, pp. 892–897, 2019.
10. Sehwag Albakri, Lein Harn, Sejun Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)," *Security and Communication Networks*, vol.2019, 2019. https://doi.org/10.1155/2019/3950129
11. Chien-Ming Chen, Xinying Zhang, Tsu-Yang Wu, "A complete hierarchical key management scheme for heterogeneous wireless sensor networks," *The Scientific World Journal,* vol. 2014, Article ID 816549, 2014.
12. Yuan, Erdong; Wang, Liejun; Cheng, Shuli; Ao, Naixiang; Guo, Qingrui., "A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks," *Sensors,* vol. 6: 1543, 2020.

13. C-T Chen, C-C Lee, I-C Lin, “Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments”. *PLoS ONE*, vol.15 (4): e0232277, 2020.
14. M.A. Simplicio, Barreto Paulo, C.B. Margi, and T.C.M Carvalho, “A survey on key management mechanisms for distributed wireless sensor networks,” *Computer Networks*, vol. 54, pp. 2591-2612, 2010.
15. Amara, said Ould, Beghda, Rachid and Oussalah, "Securing wireless sensor networks: a survey”, *EDPACS: The EDP Audit, Control and Security Newsletter*, vol.47, pp. 06-29, 2013.
16. D. Hankerson, S. Vanstone, and A. Menezes .A, “Guide to Elliptic Curve Cryptography”, *Springer Prof. Computer, Springer*, 2004H.
17. H.Chan, A.Perrig, "Random key pre-distribution schemes for sensor networks," *In Proceedings of the 2003 IEEE Symposium on Security and Privacy*, May 2003, pp.197–213.
18. L.Eschenauer, and V.D.Gligor, “A key-management scheme for distributed sensor networks,” *In: Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, Nov. 18-22, 2003*. pp. 41–47.
19. R.Blom, “An optimal class of symmetric key generation systems”, *Advances in Cryptology: Proc. EUROCRYPT ’84*, Paris, France, December 1985, pp. 335- 338.
20. F.Gandino, Cesare Celozzi, and R. Maurizio, “A Key Management Scheme for Mobile Wireless Sensor Networks,” *Applied Science*, vol. 7, no. 490, May 2017.
21. F.Gandino, B.Montrucchio, and R.Maurizio, “Key management for static wireless sensor networks with node adding,” *IEEE Transactions on Industrial Informatics*, vol. 10,no.2, pp. 1133–1143, March 2014.
22. F. Gandino, B.Montrucchio, and R.Maurizio, “Random key predistribution with transitory master key for wireless sensor networks,” *Proc. 5th Int. Student Workshop on Emerging Networking Experiments and Technology, ACM*, New York, NY, USA, pp. 27- 28, 2009.
23. W.Du, Y.S.Han, S.Chen, and P.K.Varshney, “A key management scheme for wireless sensor networks using deployment knowledge”, *In: Proceedings of IEEE INFOCOM 04. Hong Kong: IEEE Press*, March 2004, pp.586–597.
24. Hang Yan Dai, and Hongbing Xu, "Key pre-distribution approach in wireless sensor network using LU matrix," *IEEE Sensor Journal*, vol.10, no.8, pp.1399-1409, August 2010.
25. C. Blundo, A.DeSantis, and A.Herzberg, “Perfectly-secure key distribution for dynamic conference,” *Information and Computation*, vol. 1, pp. 1–23, January 1995.
26. Amar Rasheed, "Key pre-distribution scheme for establishing pairwise keys with a mobile sink in sensor network," *IEEE Transaction on Parallel and Distributed Systems*, vol.22, no.1, pp. 176-184, March 2011.
27. Liu D, Ning P, “Establishing pairwise keys in distributed sensor networks”, *In: Proceedings of 10th ACM Conference on Computer and Communications Security* (CCS03).Washington, DC, USA, ACM Press, October 2003, pp.52-61.
28. Li G, He J and Fu .Y, "A hexagon based key pre-distribution scheme in sensor networks," *IEEE International Conference on Parallel Processing Workshops,* January 2006, pp. 1-6.
29. R.Kishore, S.Radha, and S.G. Hymlin Rose, " Improved key pre-distribution scheme in wireless sensor networks using cell splitting in hexagonal grid-based de-

ployment model", *International Journal of Distributed Sensor Networks*, vol.5, no.6, pp.850-866, November 2009.

30. N.Gura, A.Patel, A.Wander, H.Eberle, and Shantz .S.C, "Comparing elliptic curve cryptography and PSA on 8-bit CPUs," *Proc. of 6th International Workshop on Cryptographic Hardware and Embedded Systems* , Boston, Massachusetts, August 2004.
31. R.Watro, D.Kong, S.F.Cuti, C.Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," *In SNSN'04: Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, New York*, October 2004, pp. 59–64.
32. X.Du, Y.Xiao, M.Guizani, and H.H.Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensors networks," *IEEE Transactions on Wireless Communications*, vol.8, no.3, pp. 1223-1229, March 2009.
33. R. M. Avanzi, and L. Tanja, "Introduction to Public Key Cryptography from Handbook of Elliptic and Hyper Elliptic Curve Cryptography", *Chapman and Hall/CRC,* Taylor and Francis, Florida, ISBN: 1584885181, July 2005.
34. F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies,* vol. 26, no. 2, pp. 107–130, 2015.
35. Danyang Qin, Shuang Jia, Songxiang Yang, Erfu Wang, Qun Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks", *Journal of Sensors*, vol. 2016, Article ID 1547963, 9 pages, 2016. https://doi.org/10.1155/2016/1547963

Figures

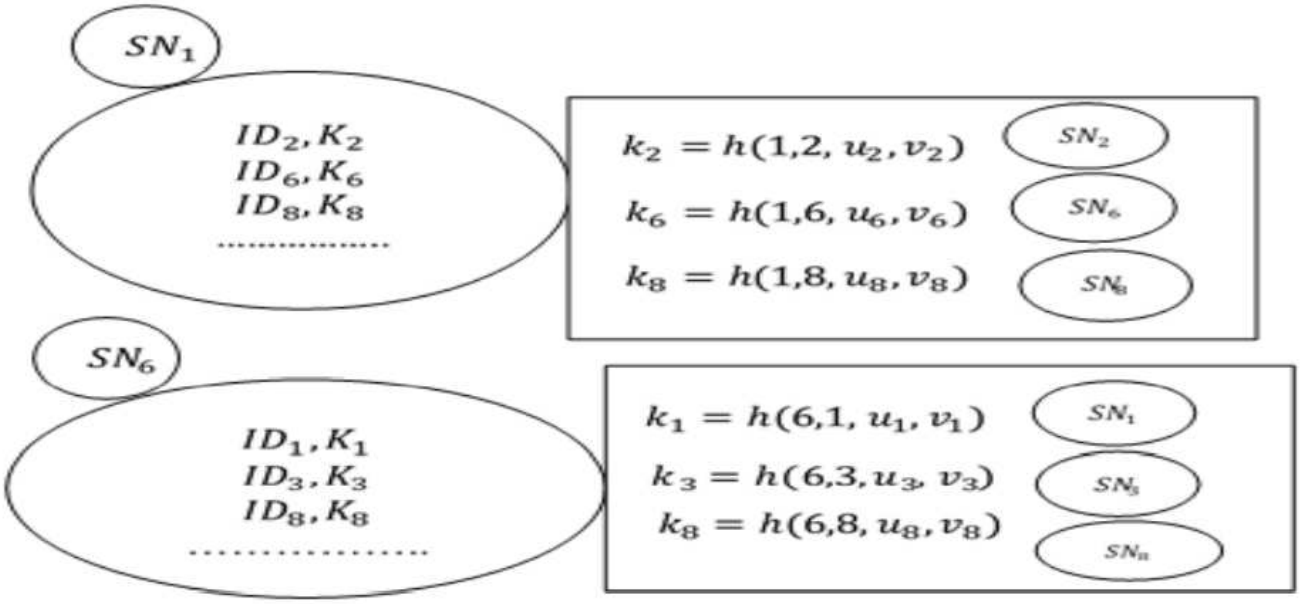

Figure 1

Key Predistribution of Hybrid Key Management Scheme.

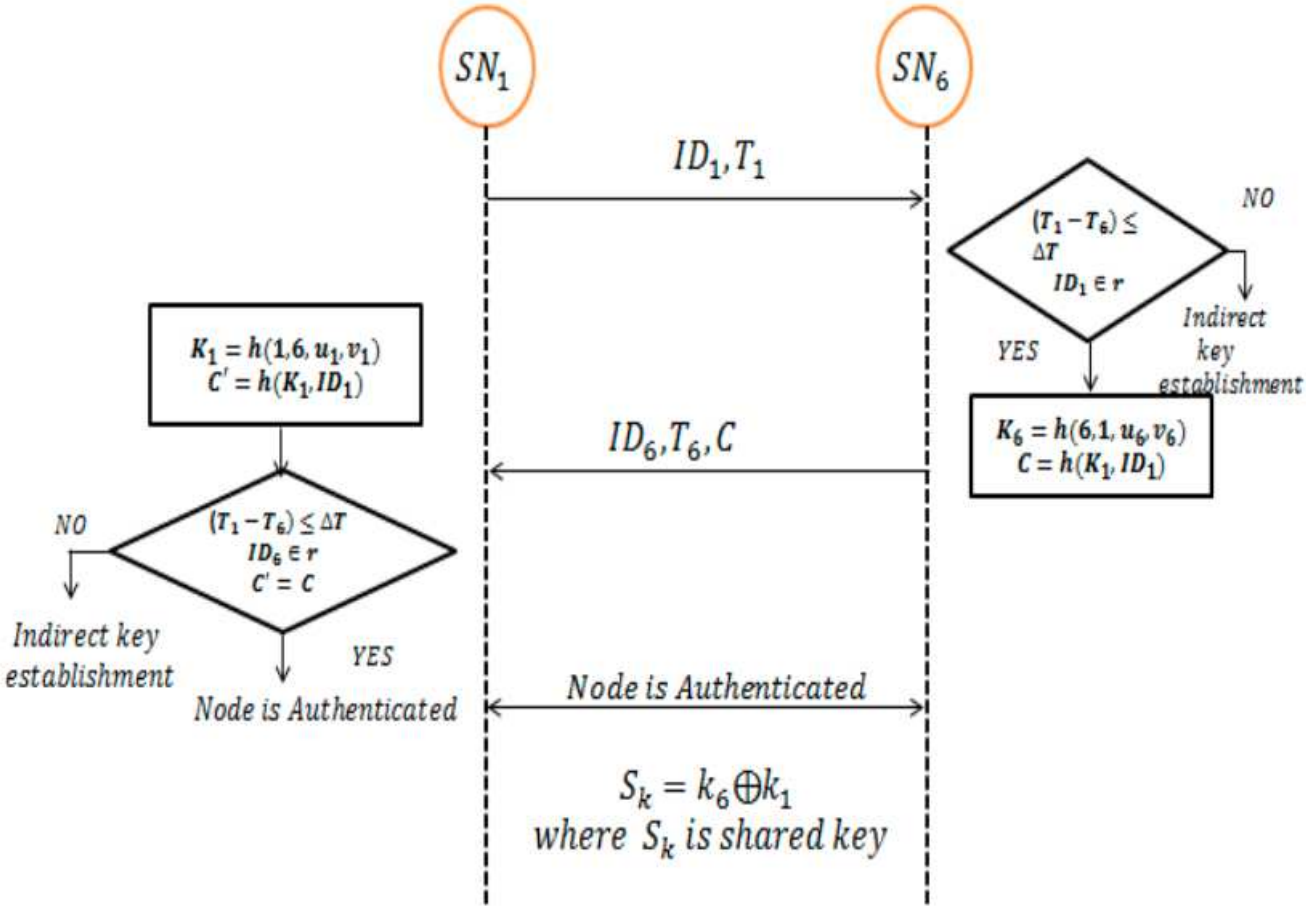

Figure 2

Direct Key Establishment between the Nodes

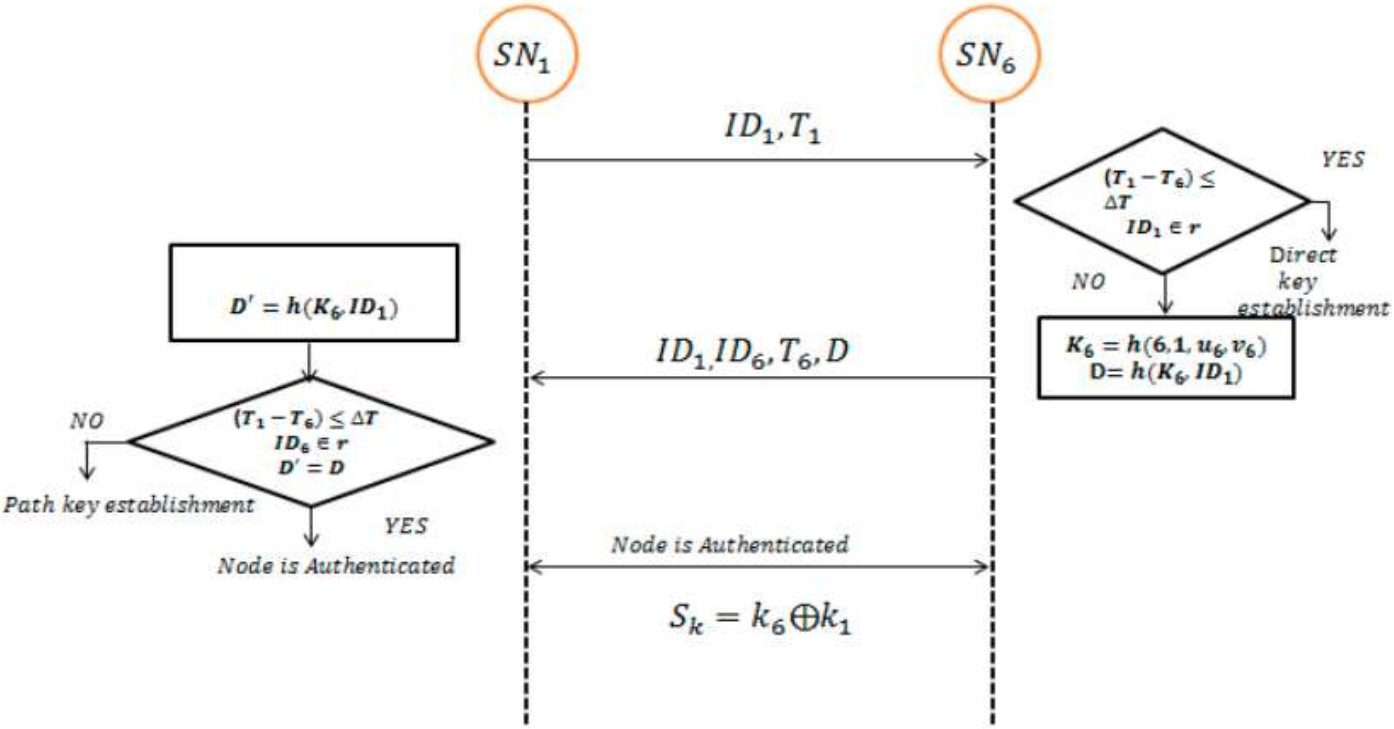

Figure 3

Indirect Key Establishment between the Nodes

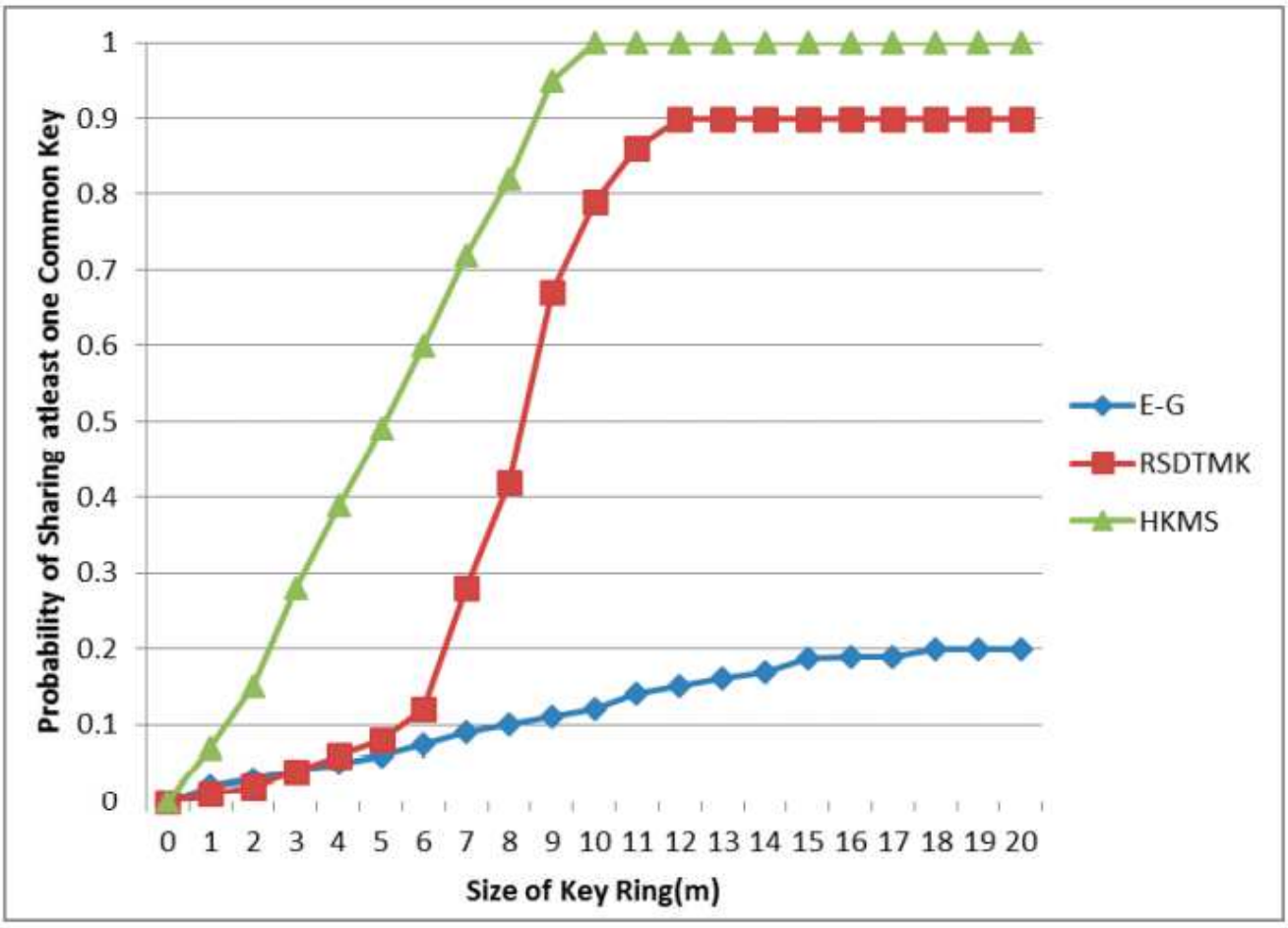

Figure 4

Connectivity Analysis of HKMS with E-G and RSDTMK

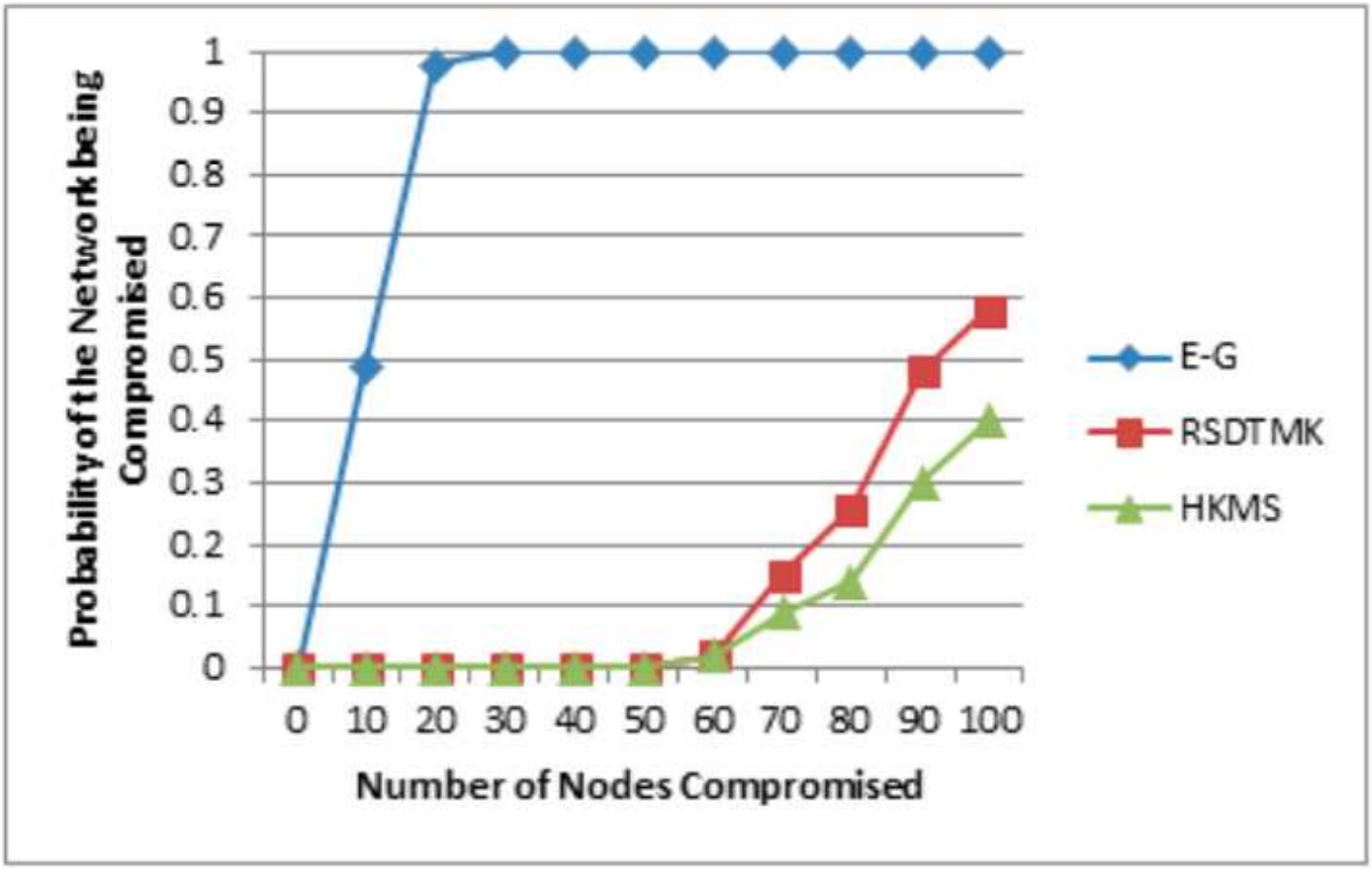

Figure 5

Connectivity Analysis of HKMS with E-G and RSDTMK

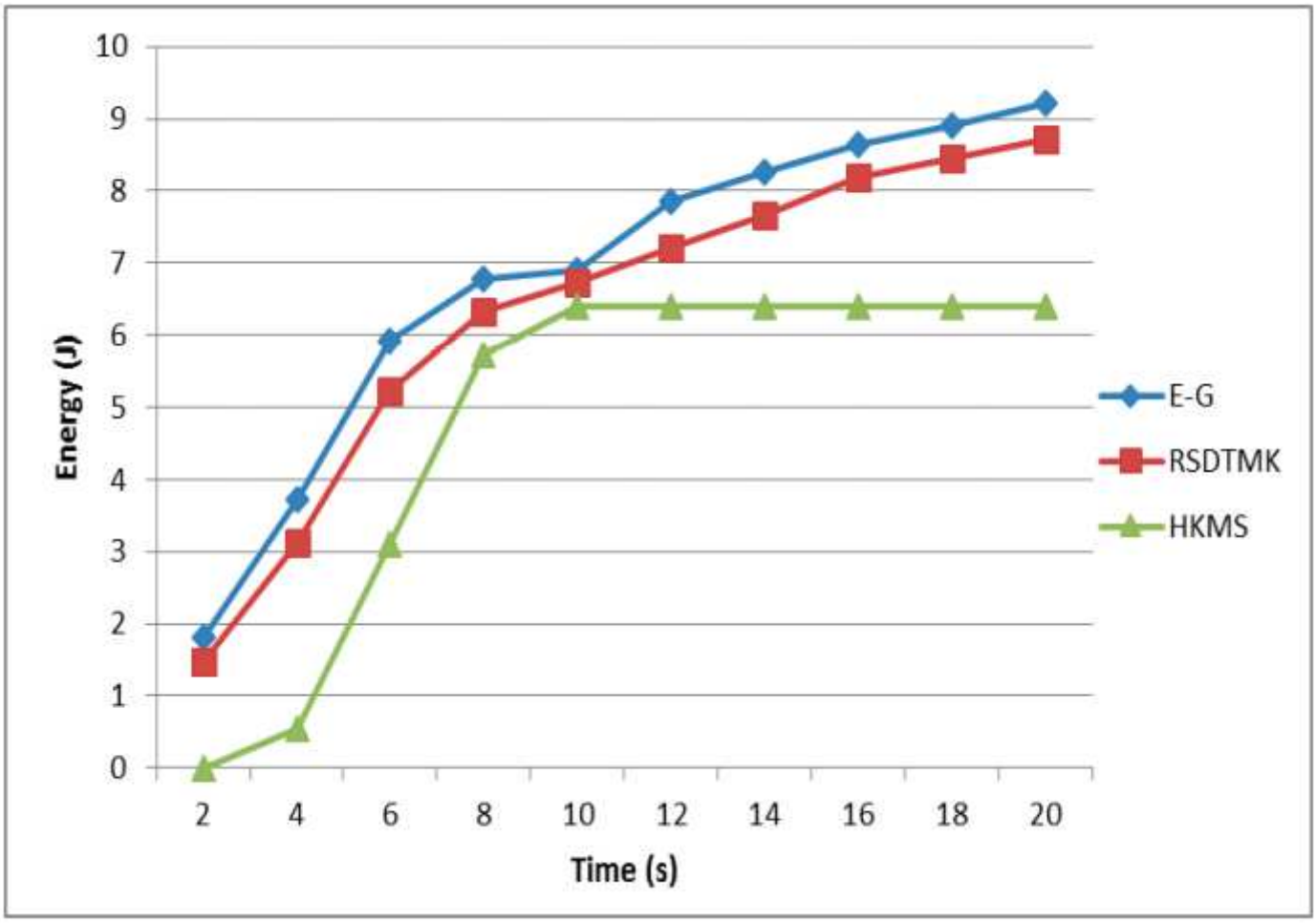

Figure 6

Comparison of Transmission Energy Consumption of HKMS with Existing Schemes

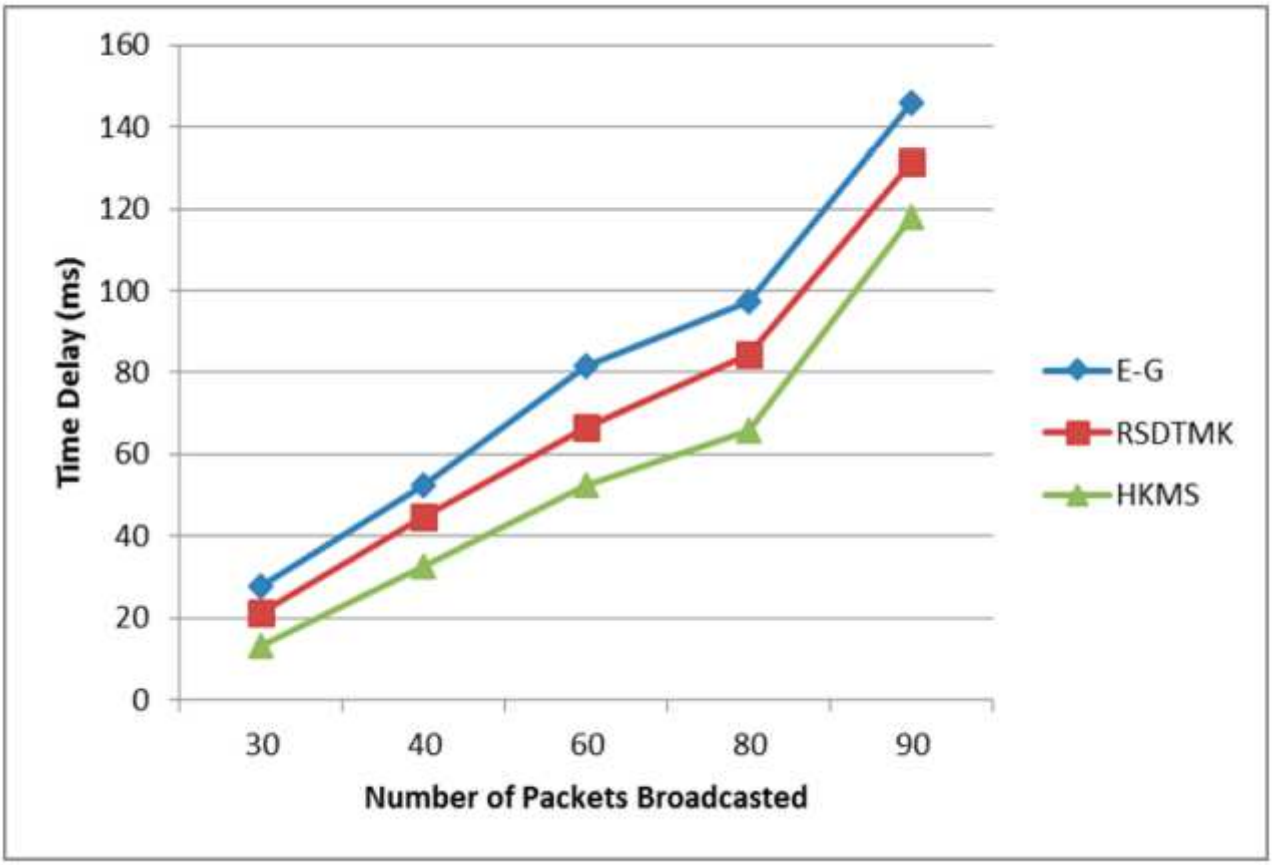

Figure 7

Packet Broadcast Delay Analysis of HKMS with E-G and RSDTMK