Unique key distribution of Secure Routing Techniques from source to destination in Wireless Sensor Networks

Ms.R.Arachanadevi	MS.R.Monica,S.Subastrika,R.Indhumathi
AP/CSE	B.E(Computer Science and Engineering)
Gnanamani College of Technology,Namakkal	

***Abstract*—In Wireless Sensor Network (WSN), secure end-to-end data communication is needed to collect data from source to destination. Collected data are transmitted in a path consisting of connected links. In End to End routing protocol, each link uses a pairwise shared key to protect data and multiple pairwise shared keys to repeatedly perform encryption and decryption over every link. This in turn increases the time complexityθ (n^2).In this project a unique end-to-end path key is used to protect data transmitted over the path also it is used to authenticate sensors to establish the path and the path key. It reduces the time needed to process data by intermediate sensors where the time complexity θ(n).**

Keywords—wsn; secure communication; group key; authentication; secreat sharing.

I. INTRODUCTION

A Wireless Sensor Network (WSN) have been deployed in various applications to collect information from human body, battle fields, smart power grids, interstate highways. Sensors are subjected by their physical limitations on hardware, storage space and computational power.The routing is the instrument of transferring information (packets) across a network from a source to a destination. The routing infrastructure needs to be established in a distributed self-organized way due to node mobility. The routing protocols are characteristically subdivided into three main categories. There are Proactive routing protocols, Reactive routing protocols and Hybrid routing protocols. Here the secure end to end routing protocol comes under Reactive routing protocol using AODV (Ad hoc On-Demand Distance Vector).An efficient solution to protect information in sensor networks is a challenging task. Here authentication service is used for security purpose. User authentication and key establishment are two fundamental security functions in most secure communications. The user authentication enables communication entities to authenticate identities of their communication partners. After users being successfully authenticated, a key establishment enables a secret session key to be shared among communication entities such that all exchange information can be protected using this shared key.

All standard paper components have been specified for three reasons: in (1) Lein Harn et al (2015) proposed a predistribution scheme for establishing group keys in WSNs. It uses a special-type of multivariate polynomial. The advantage of using multivariate polynomial can limit the storage space of each sensor, which is linearly proportional to the size of group communication. Since there is no information exchange in determining the group key, the scheme has no communication overhead in group key establishment. In addition, only polynomial computations are needed to compute the group key. In addition, they proved the security of the proposed scheme and show that the computational complexity of the proposed scheme is efficient. The proposed scheme is especially suitable in WSNs, in (2) Wenjun Gu et al (2011) designed an end to end secure communication protocol in randomly deployed WSNs. It is based on a methodology called differentiated key pre-distribution. The core idea is to distribute different number of keys to different sensors to enhance the resilience of certain links. The feature is leveraged during routing, where nodes route through those links with higher resilience. Using rigorous theoretical analysis, it is used to derive an expression for the quality of end to end secure communications, and use it to determine optimum protocol parameters. Extensive performance evaluation illustrates that the solutions can provide highly secure communications between sensor nodes and the sink in randomly deployed WSNs. They also provided detailed discussion on a potential attack (i.e. biased node capturing attack) to their solutions, and proposed several

countermeasures to this attack, and in (3) Carlo Blundolz et al (1992) proposed a key distribution scheme for dynamic conferences is a method by which initially an (off-line) trusted server distributes private individual pieces of information to a set of users. Later any group of users of a given size (a dynamic conference) is able to compute a common secure key. The theory and applications of such perfectly secure systems, in this setting, any group of users can compute a common key by each user computing using only his private piece of information and the identities of the other group users. Keys are secure against coalitions, that is, even users pool together their pieces they cannot compute anything about a key of any size conference comprised of other users. It is consider a non-interactive model where users compute the common key without any interaction. They proved a lower bound on the size of the user's piece of information to times the size of the common key. Then it establishes the optimality of the bound, by describing and analyzing a scheme which exactly meets this limitation. Then, it consider the model where interaction is allowed in the common key computation phase, and show a gap between the models by exhibiting an interactive scheme in which the user's information is only the size of the common key, and in (4) Manik Lal Das et al (2009) proposed a two-factor user authentication protocol for WSN, which provides strong authentication, session key establishment, and achieves efficiency. WSN are deployed in a confined area, which could bedivided into different zones. Authorized users can access WSNusing their mobile devices. Beforeissuing any queries to or access data from sensor network, theuser has to register with the GW-node of the network. Uponsuccessful registration, the user can submit query to the WSNat any time within a predefined or administrative configurableperiod. The basic idea of the protocol is that a user will receivea personalized smart card from the GW-node at the time of theregistration process and then, with the help of user's passwordand smart card the user can login to the sensor/GW node andaccess data from the network. The protocol is divided intotwo phases: Registration phase and Authentication phase.The proposed protocol avoids many logged in users with the same login-id and stolen-verifier attacks, which are prominent threats for a password-based system if it maintains verifier table at the GW-node or sensor node, and in (5) Sushmita Ruj et al (2013) proposed new pairwise key establishment schemes in WSN using deterministic predistribution techniques based on combinatorial designs and this design is applied for key predistribution in WSNs. A new construction of a design called strong Steiner trade and use it for pairwise key schemes in terms of security, bandwidth requirements, and applicability to both static and mobile networks. A triple key distribution in sensor networks is applied to secure routing, secure data aggregation and in communication in clustered sensor networks. We present a polynomial-based scheme and a combinatorial approach (using trades) for triple key distribution. This scheme is c-secure, where c is degree of polynomials used and is to design a secure routing algorithm using triple key, to preserve the anonymity and unlink ability of the network at the same time guaranteeing full security, and in (6) A. Shamir et al (1978) proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers. It permits secure communication to be established without the use of couriers to carry keys and it also permits one to sign digitized documents. Signature cannot be forged and a signer cannot later deny the validity of his signature. The difficulty of factoring should to be examined very closely.

II. EXISTING METHOD

In End to End routing protocol, each link uses a pairwise shared key to protect data and multiple pairwise shared keys to repeatedly perform encryption and decryption over every link.Pairwise Shared Key is every node shares a pairwise key with each of its immediate neighbors. Pairwise keys are used for securing communications that require privacy or source authentication. A pairwise shared key belonging to a node refers to a key shared only between the node and one of its direct neighbors.

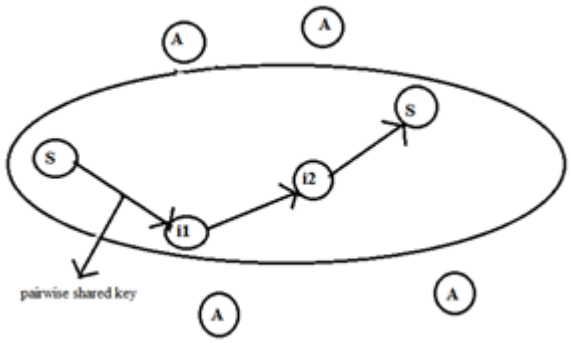

Figure1. Pairwise shared key

Pairwise Shared Key is every node shares a pairwise key with each of its immediate neighbors. Pairwise keys are used for securing communications that require privacy or source authentication. A pairwise shared key belonging to a node refers to a key shared only between the node and one of its direct neighbors (i.e. one-hop neighbours). One way for the source to distribute a message M securely to all the nodes is using hop-by-hop translation. The source encrypts M with its key and then

broadcasts the message. Each neighbor receiving the message decrypts it to obtain M, re-encrypts M with its own key, and then re- broadcasts the message. The process is repeated until all the nodes receive M.Traditional communications are one-to-one type of communications which involves only two communication entities. User authentication schemes involve only two entities, one is the prover and the other one is the verifier. The verifier interacts with the prover to validate the identity of the prover. Communication has been moved to many-to-many communications recently, also called group communications. One main concern in using a random key pre-distribution scheme to establish pairwise shared keys does not guarantee the connectivity between two sensors$\theta\ (n^2)$.

A. Problem Identified

In End to End routing protocol user authentication will authenticates one user at one time and no longer suitable for a group communication, which involves multiple users. It repeatedly performs encryption and decryption. So data transmission is delay. This in turn increase the time complexity.

III. PROPOSEDMETHOD

Secure end to-end data communication published a group key pre-distribution scheme such that there is a unique group key, called path key, to protect data transmitted in entire path. A new type of authentication called groupauthentication is proposed which can be used to determine whether all users belong to the same group or not. The group authentication is very efficient since it can authenticate all members at one time. The group authentication can only be used as a pre-processing of user authentication since if there are non-members, group authentication cannot determine who are non-members.

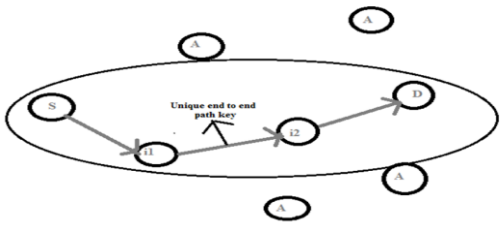

Figure 2. Unique Key

It is used to authenticate sensors to establish a routing path and to establish a path key. The main advantage is to reduce the time needed to process data by intermediate sensors and the authentication scheme has complexity θ(n), where n is the number of sensors in a communication path.

The two modules of the proposed system are classified as follows:

1. Unique Key Generation
2. Attack Prevention

A. Unique Key Generation

There is a Key Generation Center (KGC) and n sensors. There are four stages namely,

1. Key pre-distribution stage
2. Routing path establishment stage
3. Path key establishment stage
4. Data protection stage.

Stage 1: Key pre-distribution stage

Key pre-distribution is the method of distribution of keys onto nodes before deployment. The nodes build up the network using their secret keys after deployment, that is, once they reach their target position. The goal of a key pre-distribution scheme is not simply to distribute keys, but rather to distribute keys which can then be used to secure network communication. During the key pre-distribution phase, information to each node such that after deployment neighboring sensor nodes can establish a shared secret key with high probability. The KGC computes and loads keys to sensors.

Stage 2: Routing path establishment stage

At the beginning in routing path establishment stage, a path from source sensor to destination sensor has to be identified. Let $U_S$and U_D be the source sensor and destination sensor, respectively. Let the intermediate sensors identified be$U_1, U_2, \ldots, U_{m-2}$. Collected data are transmitted from $U_S$to U_D through the intermediate sensors $U_1, U_2, \ldots, U_{m-2}$. In order to establish secure group communication involving m (i.e., $2 \leq m \leq n$) sensors, it requires to authenticate all sensors in the path first. In the stage, sensors interact to prove that they are legitimate sensors. In the authentication, each sensor needs to broadcast its identity and a random integer. After receiving all identities and random integers, each sensor needs to use its secret keys obtained from the KGC initially to compute a key-hash output as its authenticationresponse. Other sensors can use this authentication response to authenticate its legitimacy. Since each sensor is required to generate an authentication response and to be verified by other sensors, the complexity of this authentication is *O(m)*.

$$AS_i = MAC(K, (i, r_i), (1, r_1), (2, r_2), \ldots., (m, r_m)) \quad (4.1)$$

AS_i = Authentication Sensor

MAC = Message Authentication Code

K=Key

$i, r_i, (1, r_1), (2, r_2), \ldots., (m, r_m))$ = Input

An authentication can also identify illegitimate sensors. At the end of authentication, each sensor knows exactly the legitimacy of other sensors in the path of secure communication. In case any sensor being authenticated unsuccessfully, a new path need to be identified and repeat this stage at the beginning. The process will be repeated until all sensors in a path have been authenticated successfully.

Stage 3: Path key establishment stage

In the path key establishment stage, a secret path key is computed first by each sensor individually. There are two keys used to protect data. One is a pair of encryption and decryption keys used by the source and the destination sensors respectively.

$$K_e = MAC(K_{1,m}, (1, r_1), (m, r_m)) \quad (4.2)$$

K_e = Encryption Key

$K_{1,m}$ = Secret Key

Another is a data authentication key used by all sensors in the path to provide authentication of the routed ciphertext.

$$K_d = MAC(K_{m,1}, (1, r_1), (m, r_m)) \quad (4.3)$$

K_d = Decryption Key

$K_{m,1}$ = Secret Key

$$K_{auth} = MAC(K, (1, r_1), (2, r_2), \ldots, (m, r_m))$$

There needs no interaction with other sensors to compute these keys. Thus, our proposed protocol is very efficient in both authentication and key establishment since there is only broadcast transmission. Furthermore, the computations of each sensor needs are polynomial evaluation and key-hash function.

Stage 4: Data protection stage

In the data protection stage, the collected data is encrypted and an authentication of the ciphertext is computed by the source sensor.

$$C = E_{ke}(data) \quad (4.4)$$

$E_{ke}(data)$ = encryption of the data using the key K_e

Each intermediate sensor needs to authenticate the ciphertext in order to forward the ciphertext to its next sensor. Unauthenticated ciphertext will be removed from this routing process.

$$Auth_c = MAC(K_{auth}, C).\{C, Auth_c\} \quad (4.5)$$

$$data = D_{kd}(C) \quad (4.6)$$

$D_{kd}(C)$ = decryption of the ciphertext using the key K_d.

At the destination sensor, the collected data can be recovered by deciphering the ciphertext.

B. Attack Prevention

An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Here, the three types of attacks have been considered.

1. Blackhole Attack
2. Eavesdropping Attack
3. Compromised Key Attack

1) Blackhole Attack

Blackhole refer to places in the network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its intended recipient. Black hole attack is a type of denial of service attack. The source node wishes to transmit data to the destination it sends a Route REQUEST (RREQ) message to all the nodes. Malicious nosed also being a part of the network receive RREQ message and replies with Route REPLY (RREP) message ahead of all the other nodes.

Here node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3.a malicious node probably drops or consumes the packets. The particular suspicious node can be regarded as a blackhole problem in network. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

It attracts additional traffic to it falsely claiming the shortest route to the destination and drops them

continuously.

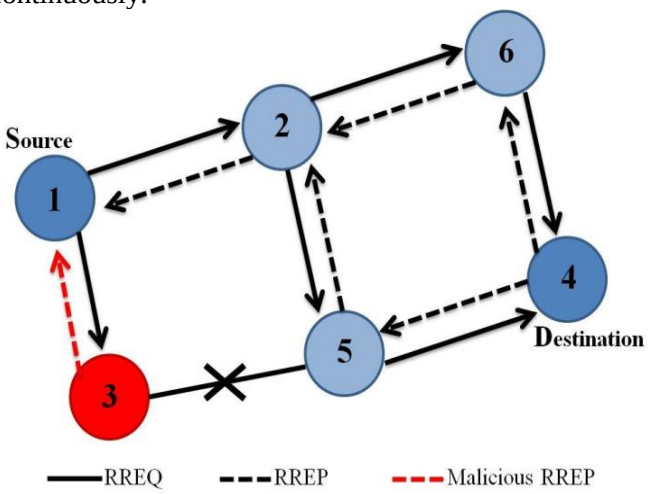

Figure 3. Blackhole Attack

2) Eavesdropping Attack

Network Eavesdropping is an attack that aims to capture information transmitted over a network by other computers. The objective is to acquire sensitive information like passwords, session tokens, or any kind of confidential information. Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, and videoconference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside.

Eavesdropping refers to the unauthorized monitoring of other people's communications. It can be conducted on ordinary telephone systems, emails, instant messaging or other Internet services. Since eavesdropping activities do not affect the normal operation of network transmission, both the sender and the recipient can hardly notice that the data has been stolen, intercepted or defaced. As the Internet has become more popular, people make use of all kinds of Internet services, for example, emails, chat rooms and social networking websites for communication. Users do not take appropriate security measures once using these communication tools, the risk of being eavesdropped will increase. Eavesdropping is as an electronic attack where digital communications are intercepted by an individual whom they are not intended.

Hacking into devices such as IP phones is also done in order to eavesdrop on the owner of the phone by remotely activating the speaker phone function. Devices with microphones including laptops and cell phones also can be hacked to remotely activate their microphones and discretely send data to the attacker. Data frames can be encrypted by encryption algorithms. An attacker can hack encrypted frames if they are not strong enough. War driving is the process of locating WLANs illegal.

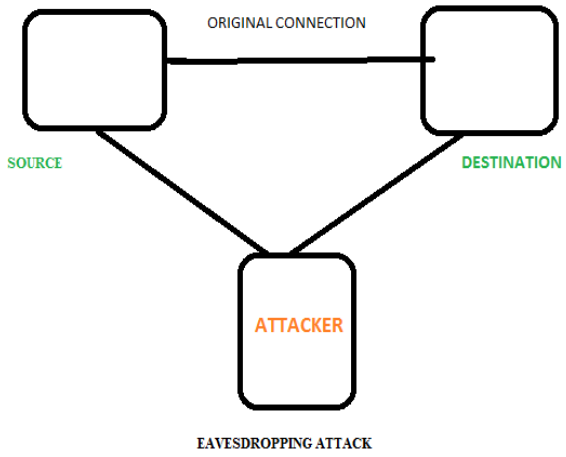

Figure 4. Eavesdropping Attack

3) Compromised Key Attack

A compromised key attack is the use of a key that an attacker has stolen to gain access to a secured transmission. The key allows the attacker to decrypt the data that is being sent. The sender and receiver are usually not aware of the attack.

A compromised-key attack occurs once the attacker determines the key, which is a secret code or number used to encrypt, decrypt, or validate secret information. The key corresponds to the certificate associated with the server. Once the attacker is successful in determining the key, the attacker uses the key to decrypt encrypted data without the knowledge of the sender of the data.

Here the compromised key attack acts as a destination node. There are two sensitive keys in use in public key infrastructure (PKI) that must be considered: the private key that each certificate holder has and the session key that is used after a successful identification and session key exchange by the communicating partners. Once the attacker is successful in determining the key, the attacker uses the key to decrypt encrypted data without the knowledge of the sender of the data.

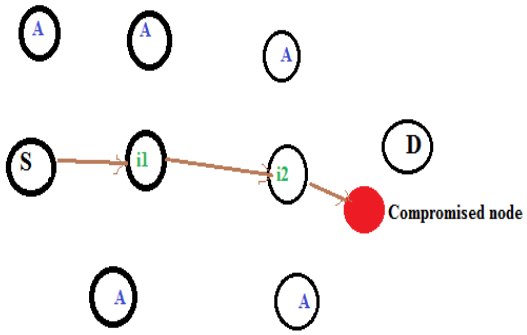

Figure 5. Compromised Key Attack

IV. RESULT ANALYSIS

The packet delivery ratio is used to evaluate the performance of attacks. Three attacks are considered here namely,

1. Black Hole Attack
2. Eavesdropping Attack
3. Compromised Attack

$$\text{Packet Delivery Ratio} = \frac{\text{Received Packets}}{\text{Send Packets}} \times 100$$

Table 1

Comparing the Packet Delivery Ratio for Blackhole Attack, Eavesdropping Attack and Compromised Key Attack.

NO.OF NODES	PACKET DELIVERY RATIO					
	BLACKHOLE ATTACK		EAVESDROPPING ATTACK		COMPROMISED KEY ATTACK	
	AT ATTACK TIME	AFTER PREVENTION ATTACK	AT ATTACK TIME	AFTER PREVENTION ATTACK	AT ATTACK TIME	AFTER PREVENTION ATTACK
10	79.9	88.6	79.2	90.3	80.5	87.9
20	77.5	89.4	79.4	90.19	77.5	89.4
30	80.8	87.5	81.38	92.45	82.8	90.4
40	78.9	90.1	79.95	93.1	78.9	89.12
50	81.3	89.5	84.5	90.3	82.7	84.9

The values of the packet delivery ratio are listed in Table 1 and Figure 6 indicates the packet delivery performance of blackhole attack in at attack time and after prevention attack. After prevention attack is improved by 8.7%.

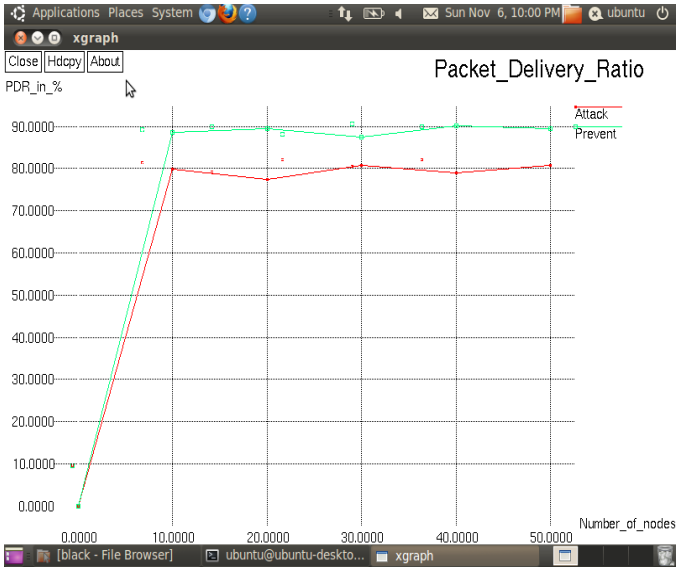

Figure 6.Comparing the packet delivery ratio for blackhole attack in at attack time and after prevention attack

The values of the packet delivery ratio are listed in Table 1 and Figure 7 indicates the packet delivery performance of eavesdropping attack in at attack time and after prevention attack. After prevention attack is improved by 11.1%.

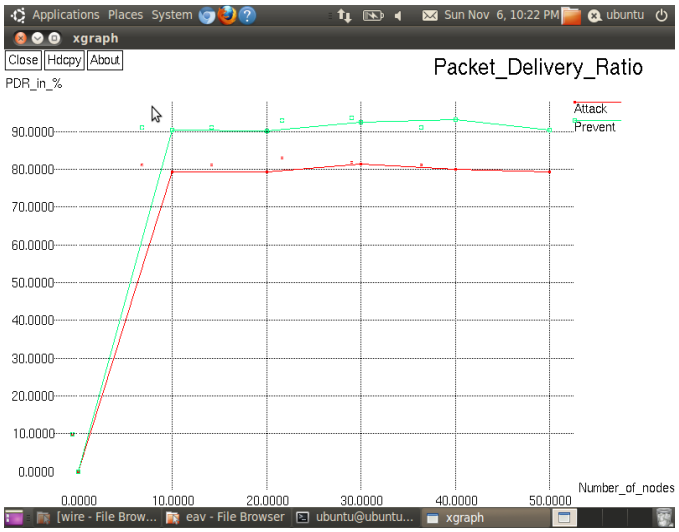

Figure 7.Comparing the packet delivery ratio for eavesdropping attack in at attack time and after prevention attack

The values of the packet delivery ratio are listed in Table 1 and Figure 8 indicates the packet delivery performance of compromised key attack in at attack time and after prevention attack. After prevention attack is improved by 7.4 %.

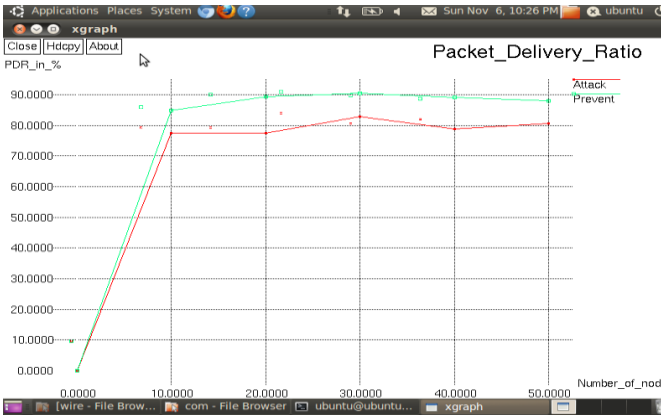

Figure 8.Comparing the packet delivery ratio for compromised key attack in at attack time and after prevention attack.

V. CONCLUSION

This project use unique path key to protect routing data by removing encryption and decryption in intermediate sensors compared to existing routing protocols which use pairwise shared key to protect routing data that required for encryption and decryption at each intermediate sensors. Three attacks namely blackhole attack, eavesdropping attack and compromised key attack have been implemented for security analysis. The performance evaluation of the packet delivery ratio is compared between before attack and after attack. Packet delivery ratio is improved by, 8.7% by eliminating blackhole attack, 11.1% by mitigating eavesdropping attack and improved by 7.4% by suppressing compromised key attack.In future, One Hop Key management method is used for secure communication. In One Hop Key management method, ECC algorithm is used which provide high level security with smaller key size.

References

[1] Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, and Yung M (1992), "Perfectly-secure key distribution for dynamic conferences", in Advances in Cryptology, Springer-Verlag, pp. 471–486.

[2] Chan H, Perrig A, and Song D (2003), "Random key predistribution schemes for sensor networks", in Proceeding of IEEE Symposium on Security and Privacy, pp. 197–213.

[3] Das M. L (2009), ''Two-factor user authentication in wireless sensor networks'', IEEE Transactions on Wireless Communications, Vol. 8, No. 3, pp. 1086–1090.

[4] Downnard I (2002), "Public-key cryptography extensions into kerberos", IEEE Potentials, Vol. 21, No. 5, pp. 30–34.

[5] D'Souza S. M. G, R. J, and Varaprasad G (2012), "Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks", IEEE Sensors Journal, Vol. 12, No. 10, pp. 2941–2949.

[6] Gu W, Dutta N, Chellappan S, and Bai X (2011), "Providing end-to-end secure communications in wireless sensor networks", IEEE Transactions on Network andService Management, Vol. 8, No. 3, pp. 205–218.

[7] Harn L and Hsu C. F (2015), "Predistribution scheme for establishing group keys in wireless sensor networks", IEEE Sensors Journal, Vol. 15, No. 9, pp. 5103–5108.

[8] Harn L and Ren J (2011), "Generalized digital certificate for user authentication and key establishment for secure communications", IEEE Transaction on Wireless Communication, Vol. 10, No. 7, pp. 2372–2379.

[9] Khan E, Gabidulin E, Honary B, and Ahmed H (2012), "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks", IET Wireless Sensor System, Vol. 2, No. 2, pp. 108–114.

[10] Ku W.C (2005), "Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture", IEEE Transactions onNeural Networks, Vol. 16, No. 4, pp. 1002–1005.

[11] Park H.A, Hong J.W, Park J.H, Zhan J, and Lee D. H (2010), "Combined authentication-based multilevel access control in mobile application for daily life service", IEEE Transactions on Mobile Computing, Vol. 9, No. 6, pp. 824–837.

[12] Ren K, Yu S, Lou W, and Zhang Y (2009), "Multi-user broadcast authentication in wireless sensor networks", IEEE Transaction on Vehicular Technology, Vol. 58, No. 8, pp. 4554–4564

[13] Rivest R.L, Shamir A, and Adleman L (1978), "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120–126.