A Dynamic Approach for Key Distribution in Wireless Sensor Network

Neetu Rani
Department of Computer Engineering, Chitkara University, Himachal Pradesh

Manik Gupta
Department of Computer Engineering, Chitkara University, Himachal Pradesh

Abstract- Sensor network is a sensing device which is used to monitor physical and environmental conditions. After monitoring the facts are distributed to main server where data is analyzed and processed. WSN mostly installed in hostile environment. Wireless sensor network has limited resource and potential applications, so safety is the major issue in the sensor network. There are various key management approaches are available to provide security in sensor network. The proposed work use SHA-512 message digest algorithm to check the authentication of new entered node and encryption, decryption process via elliptic curve cryptography. SHA-512 is a message digest algorithm. It creates message digest three times greater than SHA-1. ECC is a public key cryptography algorithm which provides higher security using small key size. The proposed work enhance the network security by increasing the network resiliency against node capture attacks and decrease the key generation time for the cluster head and for the complete network.

Keywords -- Wireless Sensor Network, Key Predistribution, Connectivity, Resiliency, Authentication.

I. INTRODUCTION

A wireless sensor network is the combination of dispersed sensors which are used to analyze physical or environmental condition like sound, pressure, temperature etc. After monitoring the sensor network pass their monitored data to main location via network. Here the data is analyze and processed. Wireless sensor network have many advantages as compared to traditional networks such as large scale, dense deployment and independent nature [1].In WSN when one node fails other nodes can collect as well as process the data thus the fault tolerance is increased .The sensor network have ad-hoc nature so it very popular in certain applications like military[2],fire detection[3], supply chain management[4], energy automation, gaming, health, environmental observation, syndrome surveillance, vision enabling and home applications [5][6][7][8][9][10][11][12][13][14].WSN used in many applications, so security of WSN is most important issue.

Security of sensor network is main challenge due to its restricted resources like power supplies, small storage, energy, computation and communication abilities. In order to provide security cryptographic approaches are used. In cryptography secret value or key is used between two entities during the transmission of data. These keys are distributed among the nodes by key management process. Key management play important role in cryptography. Key management process provides authenticity, integrity, confidentiality, flexibility, scalability to cryptographic keys. If required further these keys are modified, deleted and so on. There are various key management techniques are available for wireless sensor networks. These techniques are: (1) Single network key,(2) Trusted base station,(3) Pairwise key establishment,(4) Public key schemes,(5) Key predistribition schemes(random key predistribution technique-Composite random key predistribution technique, Polynomial pool based key predistribution,Multipath reinforcement scheme,Grid based key predistribution,Key management susing deployment knowledge, Location aware combinatorial key management ,etc.)[15].

*1. Key Predistribution***:**

There are many methods are available for creating a protected communication among nodes. The most effective method is key predistribution.In key predistribution technique certain keys are preloaded into every sensor prior their distribution. Every sensor node is allocated with a set of keys from the large key pool before deployment. After placement the two nodes having at least unique shared key, then these nodes are able to create a communication path with each other. There are lots of features of WSNs on which key predistribution methods are depends to provide the better results.

These are local connectivity, global connectivity , resiliency.

*Local connectivity***:** In local connectivity two sensor nodes should have mutual key through which they can start a protected connection for communication
*Global connectivity***:** Global connectivity is that part of nodes which is in major linked graph over the number of completely nodes.
Resiliency: Resiliency protects routes when a number of nodes are negotiated. Other issues in the strategy of WSN are hardware cost and computational cost. Hardware cost contains the cost of the battery and memory among all nodes. Computational cost is the summation of calculation completed through these phases.

Key pre-distribution techniques contain 3 stages:
Key distribution, Shared key discovery, Path-key establishment

Throughout these phases, secret keys are produced and retained in sensor entities. Then every sensor node finds another node to communicate from its communication range. A secure connection is recognized when two nodes determine one or more shared keys, these keys are dissimilar in every technique of key predistribution, then the communication is done on that connection among those two nodes. Then by joining these links paths are recognized to produce a connected graph. All the key pre-distribution approaches are divided into three ways. These are:
1) Probabilistic
2) Deterministic
3) Hybrid

In the Probabilistic approaches keys are selected on the random base and then retained into the sensor nodes. In the deterministic technique some patterns are used to choose the keys from the large pool. The hybrid method combines both the deterministic and hybrid technique to choose the keys [16].

II. RELATED WORK

There are various key predistribution techniques are created by various researchers to provide secure communication among the entities. Key predistribution is the most effective method for distributing the keys because it takes less overhead and less computation cost. Eschenauer et al [17] Develop random key predistribution technique which is also recognized as basic scheme. In this scheme keys are arbitrarily chosen from large key pool and kept in every sensor entity. Any two nodes which discover mutual keys can use these common key for safe communication.Three stages are essential for the communication keys.

A. Key Pre-Distribution:

In the key pre-distribution stage every sensor entities carries k dissimilar keys, which are arbitrarily selected from a large key pool. The key pool contains two parameters key chains L and key pool size K. The key pool contains L different key chains. The key chain is created via keyed hash algorithm. The shared-key discovery stage occurs whenever the sensor nodes are fitted into the recognized area. In this phase every node examines its neighbors in radio range with which it shares mutual keys. At the completion of shared-key discovery stage, paths are recognized among entities. Random-graph theory [18] is used in this stage to design a key pre-distribution scheme.

A.1. Shared key discovery:

When the sensor entities installed in the corresponding areas, then every sensor node examine its neighboring nodes with which it can share shared keys. The nodes transmit list of key identifier among other nodes. A protected path is recognized when two nodes find out one or more mutual keys. Then links are recognized by combining these relations to create an associated graph.

A.2. Path key establishment: Whenever two nodes are not able to exchange a mutual key then path key establishment phase provide links between two nodes. After the implementation of shared key discovery phase, number of vacant keys remains left in the sensor key ring, these keys are used by each sensor node for path key formation. The new proposed technique [19] key chain is produced via keyed hash function. The new technique provide better resiliency when associated with Eschenauer and Gligor's. This technique is considerably scalable to the bigger network zones. Random approach proposed by Eschenauer et al.is flexible, simple to employ, efficient and provide good scalability.But the disadvantage is that it cannot be deployed in environments which demand highest security.The node to node authentication is not provided by this scheme.

Chan et al proposed in [20] Q-composite technique that improves the resilience of random key predistribution. In this approach two adjacent entities can create a protected path only if they have at least Q key. This scheme use 9 mutual keys among the communication entities wherever Q is >1. Thus this scheme increases the number of keys which are shared among nodes, though it is difficult for an attacker to breakdown the network [21].

The Multipath Reinforcement technique [22] offers good security. In the basic approach the link establishments among nodes are not very much secure because the keys are selected arbitrarily from the key pool.

When one node is cooperated by the adversary the threaten nodes in the networks increase. So the value of communication keys must be modified when one entity is cooperated by the attacker.

The random pairwise key predistribution technique is the improved form of the pairwise key predistribution method. In this structure the sensor nodes are provided with dissimilar safety level and the negotiated sensor entities cannot reveal the key information in the sensor nodes which have larger security level [23].

This scheme provide unique key to each node thus it offer perfect resilience to node capture. The drawback of this technique is that it is not suitable for large size network. It is not provide good scalability.

The key predistribution using combinatorial designs are used on those applications where huge numbers of sensor nodes are deployed. In this arrangement key chains are assigned to sensor node prior their deployment. A pseudo random number is allocated to sensor nodes after their deployment [24]. In this arrangement when a new node entered in the network it was preloaded with the key which was static and the value of the key was not updated with the time. So by capturing the key any malicious node could enter in the network and capture the set of keys. The key distribution method uses the symmetric key technique which is implemented using single key. So it is not much secured mechanism. So the proposed work use a new scheme for node authentication and for key predistribution. This scheme provides better security when compared with existing work.

The paper is surveyed as in the successive text. In Section 2, the explanation of proposed framework is presented. In section 3 the simulation examination and discussions are presented. Then in section 4 the proposed scheme is compared with existing work.

II. PROPOSED ALGORITHM

The key predistribution is method of distributing key to node before their deployment in a particular environment. The key predistribution is an effective method to distributing the keys to sensor nodes because it has less computation and less overhead as compared to other key distribution techniques. The main contribution of proposed work to propose a new key distribution technique which provide improved network security related to the existing techniques mentioned above. The computations that are performed in key predistribution schemes are smaller related to that required by public key techniques. In the succeeding section we describe how to check authentication of nodes when they enter in the network and how to distribute the keys to the authenticated nodes to provide better security. Two kinds of nodes are considered in clustered hierarchical wireless sensor networks. In one type of these nodes computing power, memory and energy is high and in others small. The nodes having higher energy are considered as cluster head (CHs) and other nodes are known as cluster nodes (CNs).The cluster head can communicate directly with the base station (BS). The base station is a trusted server which is never negotiated. We present our work in two parts. The first part shows how to check the authentication of the nodes. After checking the authentication we show how to distribute key predistribution key to the sensor nodes.

A. Node Authentication-

Authentication is the principal step in any cryptographic method. One of the key features of the cryptography and internet or network security is verification. The verification creates trust by recognizing the specific system/user. There are various techniques are available to check the authentication. Traditionally a password and user ids have been used to verify. But there are numerous security disquiets in this scheme. Modern Password authentication schemes use substitutions as encoding password or by using something derived from the keyword in order to prevent them. Thus the entire idea of verification is based on secrets.

In the previous work of research the preloaded key is used to check the authentication of the node. When a node entered in the networks it was preloaded with the key that was provided by the trusted server, this key was static and the value of the key was not updated with the time. So by capturing the key any malicious node could enter in the network and capture the set of keys [24].

The proposed work provides secure method to check the authentication of new entered node. In the proposed work a trusted server is created which check the authentication of new enter node. First at the main server new node entry will be created by assigning username, password and IP address and a notepad file is created and adds to the sink node. The status is set disabled for new entered node.

Now when new node joins the cluster then IP address of cluster head is put into the node. Node checks its status from the notepad file i.e. disabled status. It means node is yet not authenticated. Further node passes its parameters to SHA512. SHA abbreviate for Secure Hash Algorithm. SHA is a cryptographic function that is created by National Security Agency (NSA). The SHA is improved form of MD4. SHA-1 creates a 160 bit message digest. The SHA contain three algorithms which are SHA-0, SHA-1 and SHA-2. The SHA-1 is much secure related to SHA-0. The SHA-512 comes after SHA-1. In SHA-2, the SHA-512 is very strong algorithm compared with other algorithms of

SHA-2. The SHA-512 creates message digest three times greater than SHA-1.Thus SHA-512 is much secure algorithm. The block size of SHA-512 has 1024 bits. Working of algorithm:

- **Padding:** The First step to implement SHA algorithm to add padding at the end of original message. So that the length of message is 64 bit short of multiple of 512.
- **Append length**: When the padding bits are added the further step to compute the original length of the message and put it to the end of message.
- **Divide the input into 1024 bit blocks**: In this step the block of input message are produced. Each block having length of 1024 bits. For the message digest process logic these blocks are working as input.
- **Initialized chaining variable**: In this step eight chaining variables are initialized from a to h.
- **Process block**: 1. Copy the chaining variable A-H into variable a-h. The combination of a-h is known as a single register, to store temporary and final result.
- 2. Divide recent 1024 bit block among 16 sub blocks, each block contain 64 bits.
- 3. SHA uses 80 rounds. Every round takes register, current block and a constant. It further update the substances of register.

Now digested message is forward to cluster head. Cluster head forward request to key server where digest message will checked against the data stored in the TPA server. If message will be match with the data stored in the key server then authenticity is provided to the new entered node. The key server will reply with big prime number and the value of prime number will also be updated in the database. Once sink node receive prime number then in the notepad file status will be updated enable and username and password are overwrite with prime number. If any cases network get down and reconnect again then node will share its prime number instead of username and password. So the proposed solution provides better security when compared with [24].

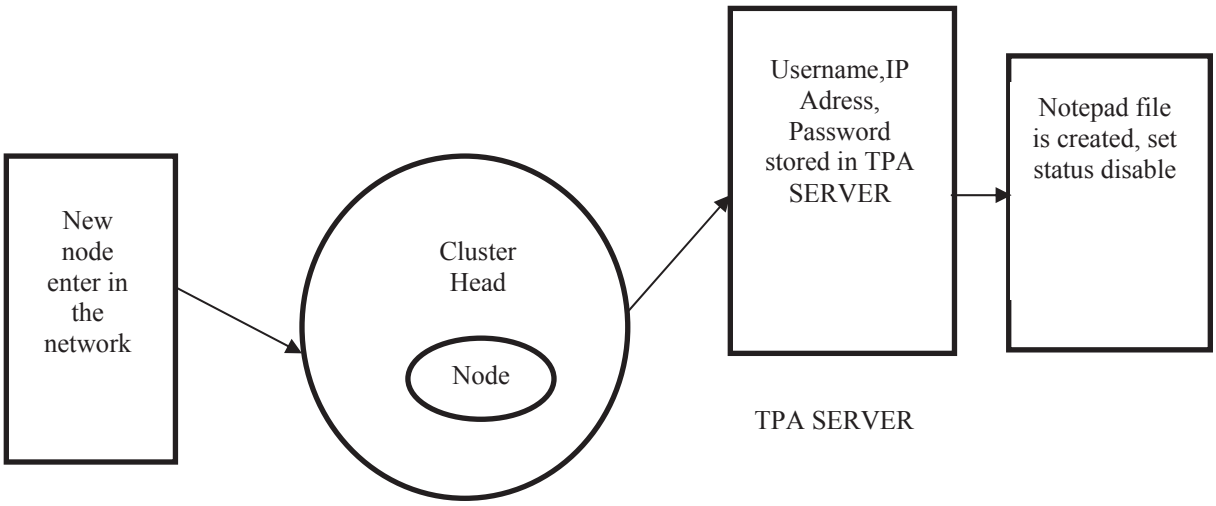


Figure1. Node Authentication

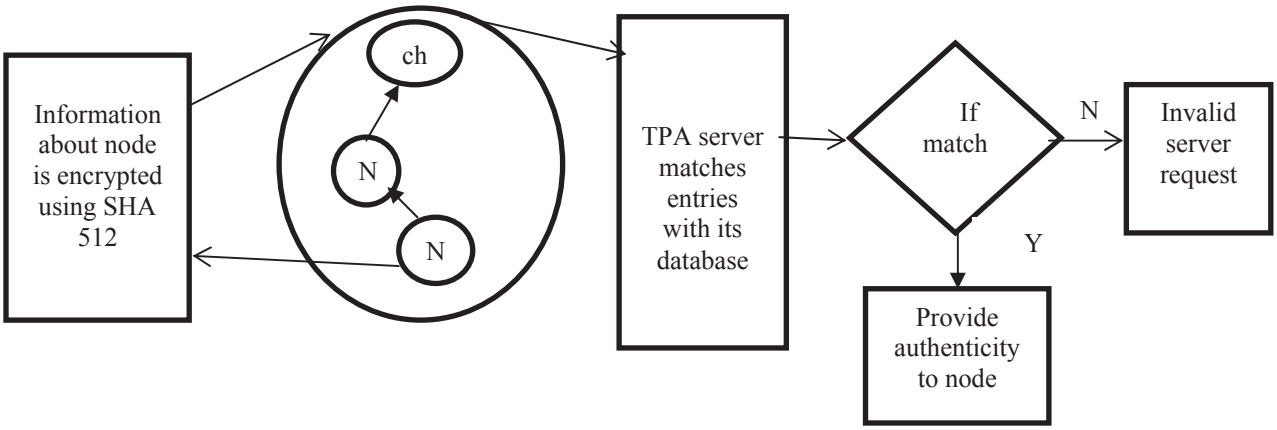


Figure 2.Flow To Check Node Authentication

B. Key Distribution-

The proposed key distribution technique use Elliptic Curve key distribution algorithm to allocate the keys among the nodes. It is a public key cryptosystem which use small key sizes. As compared with other public key schemes ECC provide much security. It has fast communication time, use less number of keys and bandwidth as compared with RSA [25]. Centered on hexagonal placement knowledge ECC contains three basic steps:
Key Generation Phase, Key pre-distribution phase, Key Agreement Phase [26].

B.1 Key generation phase

In the proposed work the authenticated nodes joins the network. When node from one cluster want to transfer data to another node placed in the diverse cluster, then it send a keyword to cluster head i.e. send file. The cluster head forward this request to TPA (which is the main server for all the clusters).Now the trusted party server create unique public key in the form of hex code for every node joined the network by using Elliptic Curve algorithm. It means the public key is different for every node in the cluster. After that node from one cluster send file to another node situated in another cluster. Again TPA server generates unique public keys for each node located in cluster 2. Along with the key a message will also forward by TPA server to CH to compute the private key. Cluster head forward this message to all the nodes present in the cluster. Now the nodes create private key from their own public key. This is the key generation phase.

B.2. Shared key discovery

After implementation of key arrangement stage, every entity wants to determine whether it shares any key with the other entity or not**.** This shared-key detection must be accomplished in every cluster among cluster nodes, among CNs and their related CHs, and between CHs. The keys create private key from the public key that is created by TPA by using Elliptic Curve formula. After this private key and IP address of the node is forward to the cluster head. Cluster head forward it to the trusted party server. All the data about the nodes is also kept in the CH. Now TPA server checks all IP address from source to destination. It means TPA server check those nodes from the different clusters which can communicate with each other. Further those keys which can communicate with each other are stored in different array. This phase known as shared key detection phase.

*B.3. Path key establishment***:**

During path key formation different paths are generated to transfer the data from one node to another. In the proposed work during path key establishment when authenticated node wants to transfer the data to another node situated in different cluster. Then firstly this node connected with another authenticated node which is present in the network, further this node connected with another authenticated node and so on. After this path is connected with CH, CH forward to TPA server. Now TPA server transfer file to CH of another cluster. Cluster head forward file to destination node. Here destination node decrypts the file.

In the proposed work to maintain the security of keys the trusted party server update the key after few seconds and broadcast the message to all entities that are entered in the network. The nodes revert back to TPA server about getting the updated key, any node which can't revert back to TPA server declare unauthorized node and it is blocked

by trusted party authenticated server. So the proposed work enhances the security by updating the keys after a few seconds.

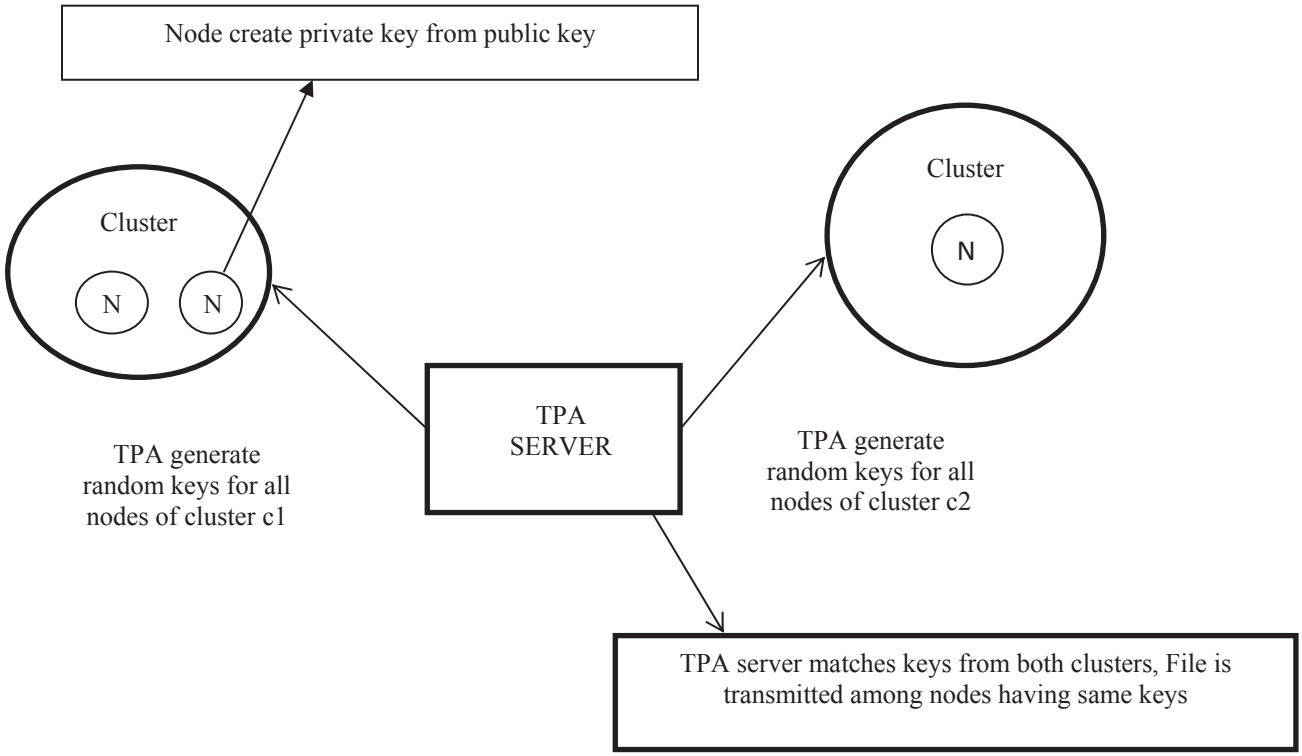


Figure 3.Key Generation

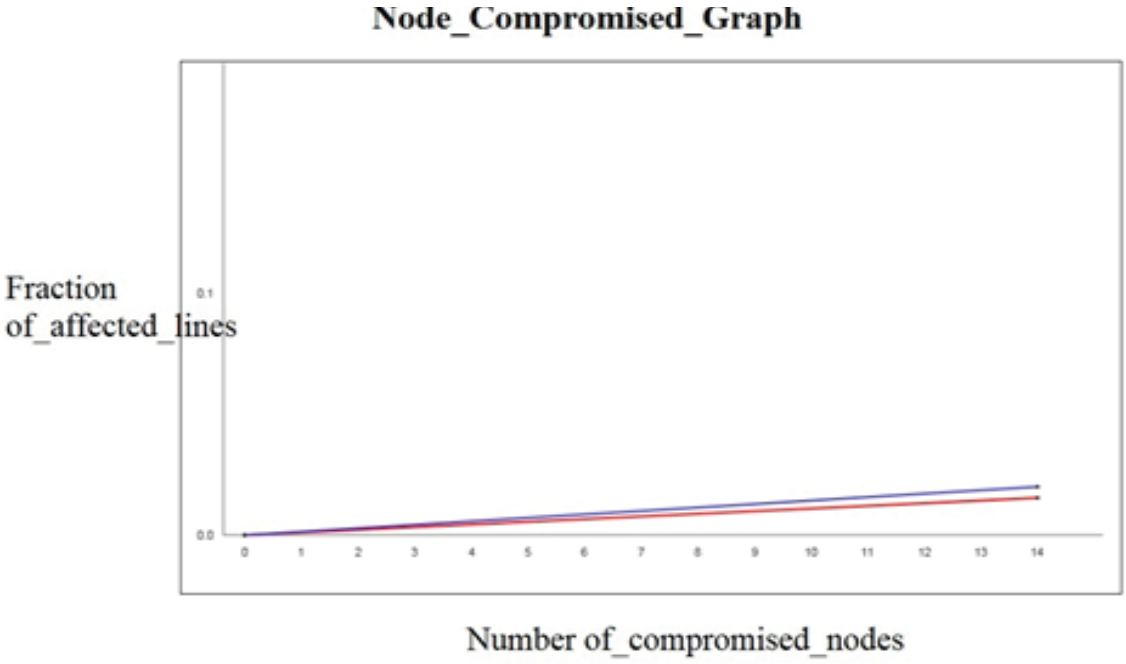
III. Experiment and Result

In this segment we examine the security and performance of our technique. The results of the proposed work are compared with the factors: Resiliency, key generation time.

1. Resiliency: Once sensor nodes are dispersed, some of them may be cooperated via attacker. In this situation, we suppose that whole number of keys or information kept on captured nodes can be sensed by the challenger. So, exposed keys cannot be used further for protected communications among entities. Also links having exposed keys will be in danger. The resiliency of a network is defined as the probability of a link between two uncompromised nodes is broken, when s nodes are captured, which is denoted by fail(s).Thus the resiliency is the capacity of a network to continue operate in presence of K compromised node. By taking the weighted average on all clusters the resiliency of complete system is calculated.

Fail = Number of damaged links /Total number of links between uncompromised entities.

The main aim of proposed work is to provide high resiliency by distributing the keys in a secured manner. For this the secure key is distributed after a few seconds to all the nodes entered in the cluster. The proposed scheme offer high resilience compared with existing work.

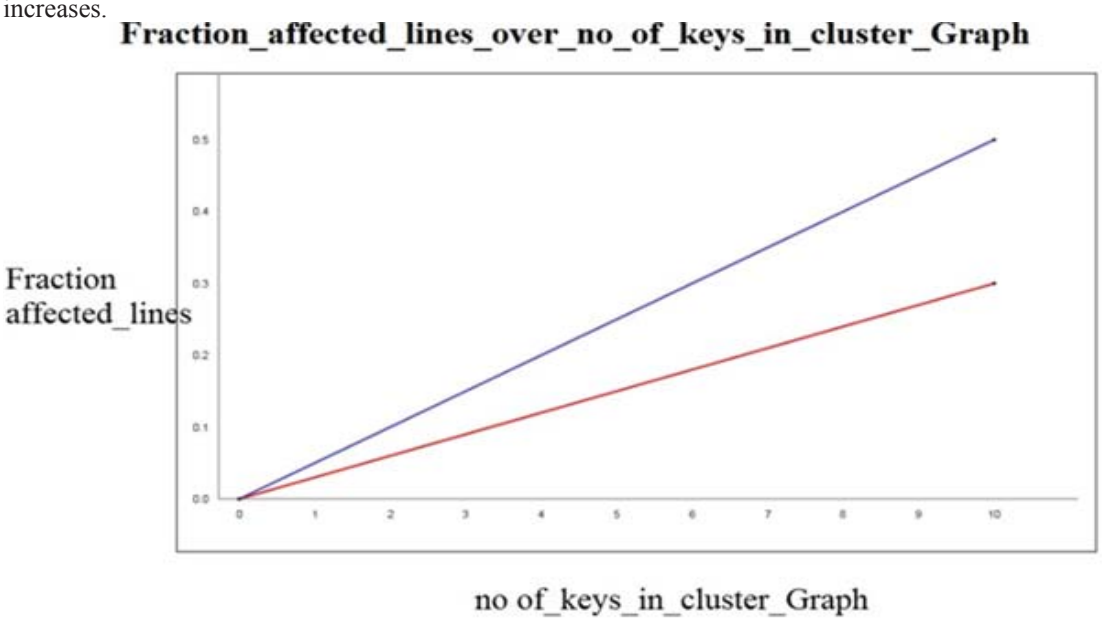


Research Value [14.0, 0.0154]

In the proposed work when 14 nodes are compromised then the ratio of affected lines is 0.0154.

Thus the proposed works provide high resiliency when compared with existing work [24]. This resiliency enhancement is due to updation of key.

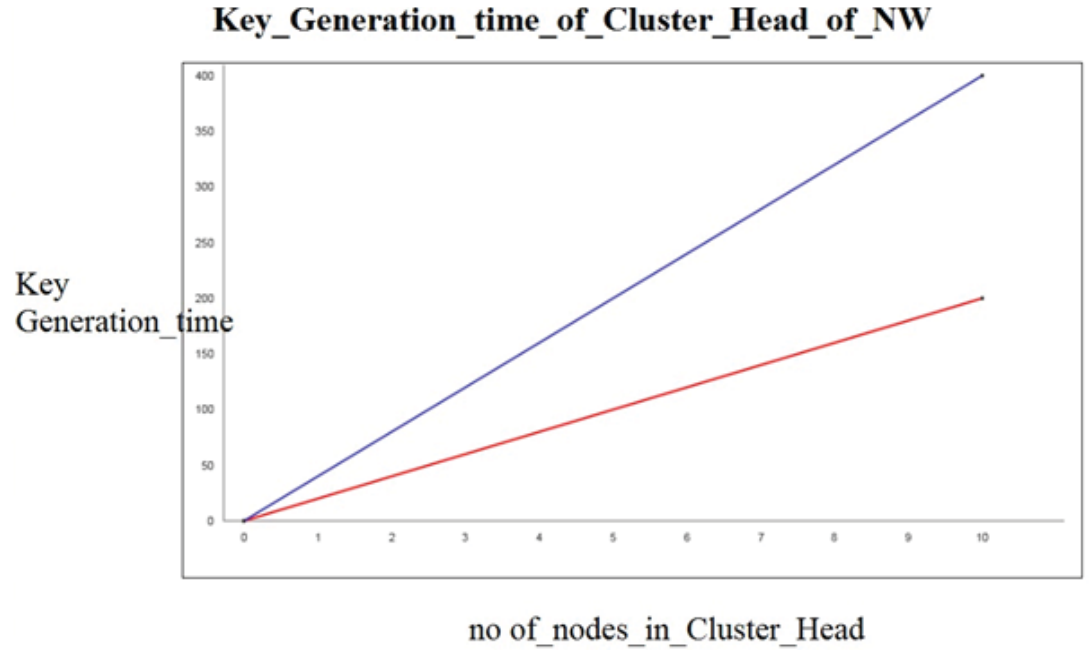
Furthermore, the proposed works display what is the effect on resiliency when the number of clusters increases in the network. The curves in the following figure illustrate the value for fail(s) by increasing volume of clusters increases.

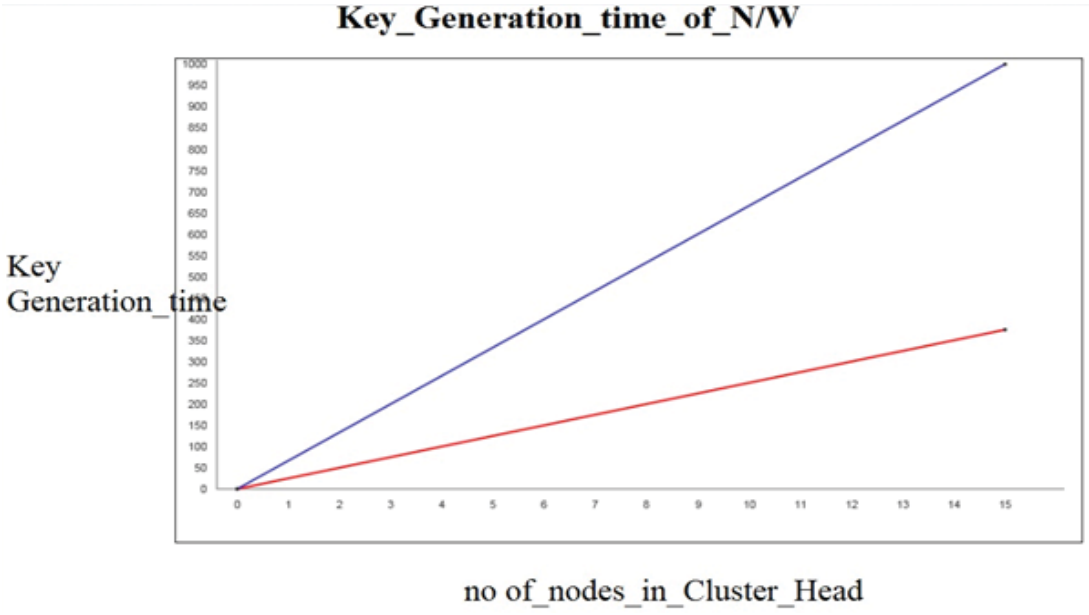


Research Value [10.0, 0.3]

Obtained result determines that the resiliency of the network can be significantly enhanced by growing the quantity of clusters.

2.Key generation time**:** The key generation time of the proposed work is discussed in this section. The proposed key generation time is compared with [27]. Both key creation algorithms are executed on a system with Intel core duo, 3.20 GHz processor speed, and 4-GB RAM. The result graph shows that when the number of entities in the network increases then the key creation period is also increased. The comparison shows that the proposed scheme provides fast results. The succeeding figure display the key creation time in cluster head and in whole network.





IV. COMPARISON

The proposed scheme use SHA-512 message digest algorithm to check the authentication of the node and elliptic curve public key algorithm to distribute the keys among the nodes in a predistribution manner. The proposed work enhances the security by updating the keys after few seconds. For node authentication SHA-512 algorithm is used which is very much secure as compared with another message digest algorithms. The ECC algorithms provide the higher security by using small key size. Thus the proposed research provides very high resiliency and decrease the key creation time for the whole network and for the cluster head

A. Comparison with existing schemes in [24] and [27]

In [24] a preloaded key is used to check the authentication of the node. When any node enters in the network it was loaded with preloaded key. Thus the only scenario is that if any node having preloaded key then it can join the network. It was not so much secure method to check the authenticity of the new entered node because the value of preloaded key was fixed and was not updated with time. So any malicious node could enter the network by capturing the preloaded key and could gradually capture the network key set by sniffing the network.

Also, the key distribution mechanism uses the symmetric key technique that is implemented with single key. This could be captured easily if the key set was already compromised by the adversary. So to enhance the security in proposed work SHA-512 message digest algorithm is used to check the authentication of the nodes and elliptic curve the public key is used to distribute the keys among the nodes. The proposed scheme enhances resiliency and decrease the key generation time when compared with [24] [27].

V.CONCLUSION

The key Management techniques for WSN are active research area. It offers significant security for sensor network. The proposed work checks the authentication of new entered node by using SHA -512 message digest algorithm. SHA-512 is very secure when compared with other SHA-2 algorithms. The key mechanism use elliptic curve public key which is very secure. It provides higher security using small key size. Thus the key size takes less memory. The proposed work enhances the security of the network by increasing the resiliency of the network against node capture attacks. It also decreases the key generation time for the cluster head and the key generation time for the complete network. Furthermore, the transactions can be reduced when to digest the message and forward to base station to check the authentication of the node. The network security can be enhanced when keys create private key and forward to cluster head by using another key predistribution technique.

REFERENCES

[1] S.U. Rehman, M. Bilal, B. Ahmad, K. M. Yahya, A. Ullah, O. U. Rehman," Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN), IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, Jan. 2012.

[2] C.K. Chang, J. M. Overhage, J. Huang "An Application of Sensor Networks for Syndromic Surveillance" 2005 IEEE

[3] Y Dunfan.,DaoliGong,WeiWang "Application of Wireless Sensor Networks in Environmental Monitoring", 2009 2nd International Conference on Power Electronics and Intelligent Transportation System.

[4] Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi "Application of Wireless Sensor Networks in Energy Automation", Sustainable Power Generation and Supply, 2009. Supergen '09. International conference.

[5] Sundip Misra, Vivek Tiwari and Mohammad S. Obaidat, Fellow, IEEE "LACAS: Learning Automata-Based Congestion Avoidance Scheme for Healthcare Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, May 2009.

[6] I. F. Akylidiz, T. Melodia, , K. R. Chowdhury, "Wireless Multimedia Sensor Networks: Applications and Testbeds", Proceedings of the IEEE. Vol. 96, No. 10, October 2008.

[7] K. Kim, J. Jun, S. Kim, B. Y. Sung "Medical Asset Tracking Application in Wireless Sensor Networks", The Second International Conference on Sensor Technologies and Applications IEEE, 2008.

[8] N. Rajendran, P. Kamal, D. Nayak, S. A. Rabara, " WATSSN: A Wireless Asset Tracking System using Sensor Networks", Proceedings of IEEE International Conference On Personal Wireless Communications, Jan 2005.

[9] G. W. Allen, K. Lorinca, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, "Deploying a Wireless Sensor Network on an Active Volcano", IEEE Internet Computing, IEEE Computer society, March/April 2006.

10] K. Chintalapudi, T. Fu, J. Paek, N. Kothari, S. Rangwala, J.Caffrey, R. Govindan, E. Johnson, "Monitoring Civil Structures with a Wireless Sensor Network", IEEE Internet Computing, IEEE Computer society, March/April 2006.

[11] I. Ituen, G. Sohn, "The Environmental Applications of Wireless Sensor Networks", International Journal of Contents, Vol.3, No. 4, Dec 2007.

[12] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", WSNA'02, Sep 2002

[13] A. Rowe, D. Goel, R. Rajkumar "FireFly Mosaic: A Vision-Enabled Wireless Sensor Networking System", 28th IEEE International Real-Time Systems Symposium,2007.

[14] E. Sazonov, K. Janoyan, R. Jha, "Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring", Proceedings of Structural Materials Technology (SMT): NDE/NDT for Highways and Bridges, 2004.

[15] Y. Xiao, V. K Rayi, Sun, X. Du, Fei Hu, M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks" Journal computer communications, Vol. 30, No 11-12, pp. 2314-2341,2007.

[16] Neetu Rani and Manik Gupta,"review on key predistribution schemes in wireless sensor networks", International Journal of Advanced Smart Sensor Network Systems (IJASSN), Vol 6,No.1, January 2016.

[17] Escenauer L,Gligor vd, a key management scheme for distributed sensor networks", conference on computer and communication security proceedings of the 9th ACM conference on computer and communication security,Washington,DC,USA, 2002.

[18] ,J. Spencer,"The Strange Logic of Random Graphs, Algorithms and Combinatorics", NO.22, Springer- Verlag,2000.

[19] Kui Ren, Kai Zeng , Wenjing Lou,(2006)" A newapproach for random key pre-distribution in large-scale wireless sensor networks", wireless communications and mobile computing, Vol 6,No 3 ,pp.307-318.

[20] H. Chan, A. Perrig, D. Song, "Random key predistribution schemes for sensor networks, " in IEEE SP, pp. 197–213,2003.

[21] S.Sibi, A. R Thamizarasi,(2013), "Key Pre-Distribution Methods of Wireless Sensor Networks" International journal of Scientific & Engineering Research, Vol 4, No 11.

[22] J.Deng ,Y.S.Han , "Multipath Key Establishment for Wireless Sensor Networks Using Just-EnoughRedundancy Transmission" IEEE Transactions on Dependable and Secure Computing, Volume 5, No 3, pp. 177-190,2008

[23] S.B.Wicker,M. J. Bartz,(1994)"Type-II hybrid-ARQ protocols using punctured MDS codes",IEEE Trans. on Communications, vol. 42, no. 2/3/4, pp. 1431–1440

[24] M. Javanbakht,H.Erfani, H.H. S.Javadi , P.Daneshjoo, "Key Predistribution Scheme for Clustered Hierarchical Wireless Sensor Networks based on Combinatorial Design", Published online in Wiley Online Library, Vol. 7, No 11, pp. 2003–2014,2014

[25] A.S. Wander, N. Gura, H. Eberle et al., "Energy Analysis of Public – Key Cryptography for Wireless Sensor Networks,"in Proc. of the 3rd International Conference on Pervasive Computing and Communications (PERCOM), 2005.

[26] Y.Kumar,A.Nageswara Rao," Secure Communication through Prior Key Distribution System for Nodes", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 4, September 2014.

[27] S. K. Sahoo, M. N. Sahoo," An Elliptic-Curve-Based Hierarchical Cluster Key Management in Wireless Sensor Network", Intelligent Computing, Networking, and Informatics, Springer India, pp.397-408, 2014

.

.

.