ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

Secure and Efficient Protocols with Key Management in Dynamic Wireless Sensor Network

Ahmed Abdulhasan Jinah

Student, Department of Computer Science, DR.D.Y Patil College, Pune, India

ABSTRACT: Recently, wireless sensor networks (WSNs) have been established for vast diversity of applications such as military tracking, health care monitoring, traffic monitor-ing, where sensor nodes are frequently move from different locations. Secure data transmission in wireless sensor network is challenging task. A good encryption key management protocol is required to secure data and communication. Clustering is a novel approach and practical way out to increase the system performance of WSNs. Proposed system presents a effective key management to secure data transmission for WSNs, in which the clusters are designed. Proposed work present two secure and efficient data transmission protocols for WSNs, called IBS and IBOOS, by using the identity-based digital signature (IBS) technique and the identity-based online/offline digital signature (IBOOS) scheme, respectively.In IBS, network security depends on the use of the Diffie-Hellman problem in the pairing domain. SEDT-IBOOS re- duces the computational overhead for protocol security, which is important for WSNs, while its security depends on the wireless network design. Proposed system show the feasibility of the effective key management with SEDT-IBS and SEDT-IBOOS pro- tocols with use of security requirements and security analysis against various attacks such as passive attack, known key attack and impersion attack.We have discussed a novel integrated approach of IBS and IBOOS for effective key management. We have provided experimental evaluation of the proposed protocol through simulation results.

KEYWORDS: Wireless sensor networks, IBS, IBOOS, keymanagementscheme.

I. INTRODECTION

A Wireless Sensor Network (WSN) is a distributed network of small sensor nodes deployed in large numbers to monitor the environment or other systems by the measurement of physical parameters such as temperature, pressure, or relative humidity. These nodes by monitoring, collects the detailed information about the physical environment in which they are installed, then transmits the collected data to the Base Station (BS). BS is a gateway from sensor networks to the outside world. The BS has a very large storage and large data processing capabilities. It passes the data it receivesfromsensornodestotheserverfromwhereend-usercanaccessthem.The sensors nodes are generally deployed around the area of the BS. A straightforward method to collect the sensed information from the network is to send each sensor nodes reading to be forwarded to the basestation, via other intermediate nodes, before the base station processes the received data. However, this method is expensive in terms of communication overhead, which prompted active research to design an energy-efficientmechanism[1,2].Infig.1.1,agenericWSNscenarioisshowninwhich therearesevenclustersandsensornodesaredistributedineachcluster.Thesensor nodes are sending the sensed data to BS in multi-hop fashion via cluster head to cluster head. In this architecture there are multiple sources and one destination.

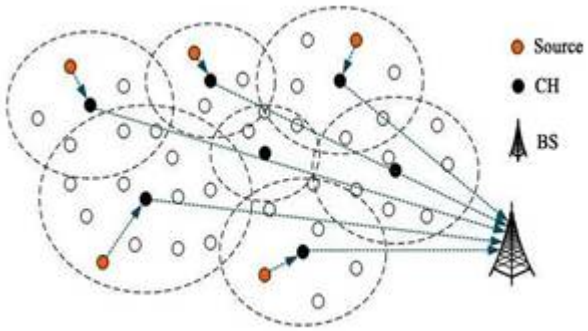
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018



A sensor node is made up of four basic components such as sensing unit, processing unit, transceiver unit and a power unit which is shown in fig. 1.2. It also has appli- cation dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sen- sors and analogue to digital converters (ADCs)[4].The analogue signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit is generally associated with a small storage unit and it can manage the procedures that make the sensor node collaborate with theothernodestocarryouttheassignedsensingtasks.Atransceiverunitconnectsthe node to the network. One of the most important components of a sensor node is the power unit. Power units can be supported by a power scavenging unit such assolar cells. The other subunits, of the node are application dependent. This is very common structure of sensor node which is used inWSN.

II. LITERATURE SURVEY

Name of the paper	Author name	Proposed scheme and Disadvantages
1] Effective key management in dynamic wireless sensor network-2015	eung-Hyun Seo, Jongho Won, Salmin Sultana	Proposed a CL-EKM scheme, which also provides forward and backward secrecy.
2]Random Key predistribution schemes for sensor networks- 2015	Adrian Perrig Dawn Song	Focused on bootstrapping problem in resource constrained sensor network.
3]A key predistribution scheme for sensor networks using deployment knowledge-2014	Pramod K. Varshney	Advantage of the prior knowledge about deployment and reduces the number of unnecessary key spaces carried by each sensor.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

4]EDDK:Energy efficient distributed deterministic key management for WSN-2012	X. Zhang, J. He, and Q. Wei	Proposed a distributed deterministic key management based on ECC. It uses symmetric key for existing node and asymmetric for new node. Not secure against known key attacks.
5]An efficient key management for WSN-2012	D. Du, H. Xiong, H. Wang	Uses a ECDSA scheme to verify identity of cluster head and static EC-Diffie-Hellman key agreement scheme to share the pairwise key between cluster heads. Not secure .
6]First authenticated key establishment protocol for self organizing sensor networks-2010	Q. Huang, J. cukier, H. kobayshi	Proposed a ECC based key establishment scheme for self organizing WSN. Security weakness: sensor node's private key is exposed to other node during key establishment.
7]A novel key update protocol in mobile sensor network-2014	S. Agrawal, R. Roman, M. L.Das, j.Lopez	Proposed a two layered key management scheme and a dynamic key update protocol in D WSN based on Diffie Hellman.
8]Dynamic and secure key management model for hierarchical heterogeneous sensor network-2013	M.R. Alagheband, M.R. Aref	Proposed ECC, base station is suffers from more overhead of certificate management, not secure

III. PROPOSED METHODOLOGY & DISCUSSION

1. Objective ofsystem

The objective of this proposed system secure data transmission along with key man- agement.

1. To secure data transmission by using advantage of IBS and IBOOS protocols.
2. To reduce the delay of the system, and to increase the throughput rate by measuring the successful delivered packet through the transmission.
3. To reduce the transmission overhead of shares by using Key management.
4. Robust path finding and pathreconstruction.
5. To reduce the energy consumption of proposedsystem.

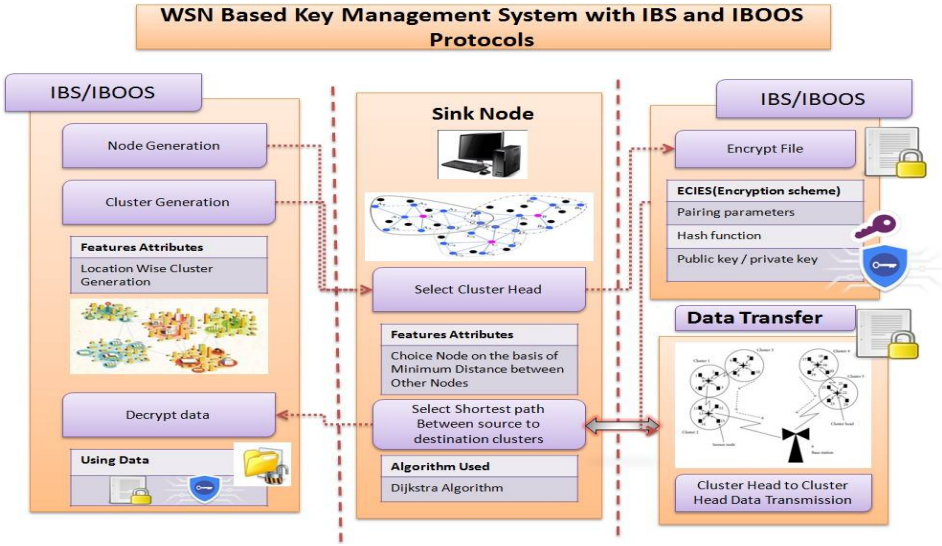
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

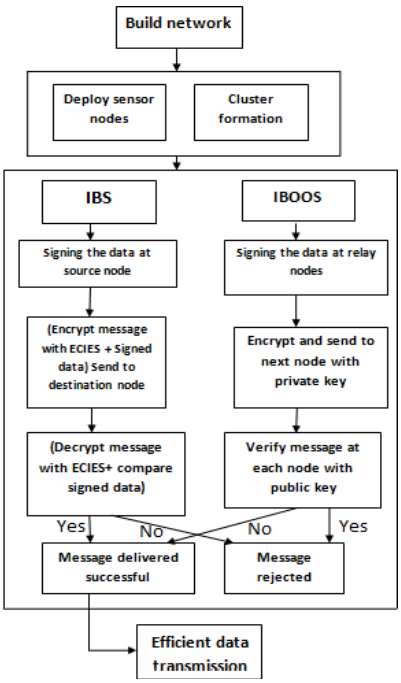
Vol. 7, Issue 5, May 2018



Proposed system architecture diagram

2.Proposedsystem

The proposed architecture of our system is shown in figure 2.1. Proposed architecture address the problem for security verification with using key management. In this pro- posed system different key management techniques are used which includesindividual key, pair wise key, cluster key, public key private key cryptography for effective and secure keymanagement.



Proposed system design

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

ALGORITHMS

1. RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can begiven to everyone.

2. SHA Algorithm

Acryptographichashisakindofsignatureforatextoradatafile.SHA-256generates an almost unique 256 bits signature for a text. A hash is not encryption; it cannot bedecryptedbacktotheoriginaltext.

3. ECIES algorithm:

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receivers public key and the receiver will decrypt its privatekey.

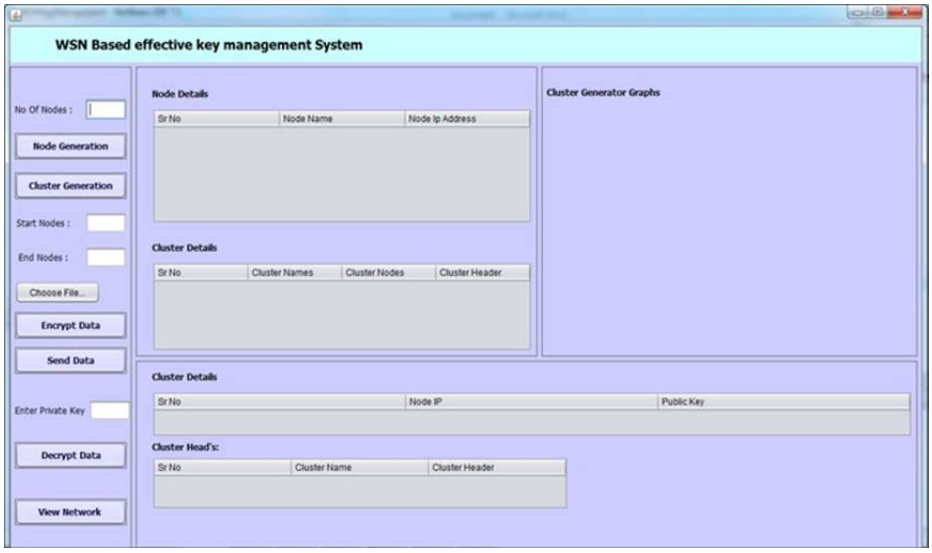
4. Routing Algorithm:

For each visited node u, dist[u] is the shortest distance from source to u; and for each unvisited v, dist[v] is the shortest distance via visited nodes only from source to v (if such a path exists, otherwise infinity; note we do not assume dist[v] is the actual shortest distance for un-visitednodes).

IV. EXPERIMENTAL RESULTS

1. Initialize network

The very first step of system, where we have to give the number of nodes in the network, after that select source and destination to send a message. After selecting the source and destination, select the file which we have to send and click on encrypt to encrypt that file. Then click on show network to create a network.



2. Message encryption

After formation of clusters in a network, the CHs brodcast the clus- ter information which includes the cluster key, information about new node addedand node deletion. Then all nodes generate its own private key with help of individual key, which is used to encrypt message. The pairwise key and cluster are also gener- ated while sending message from source to destination. The figure shows message is successfullyencrypted.

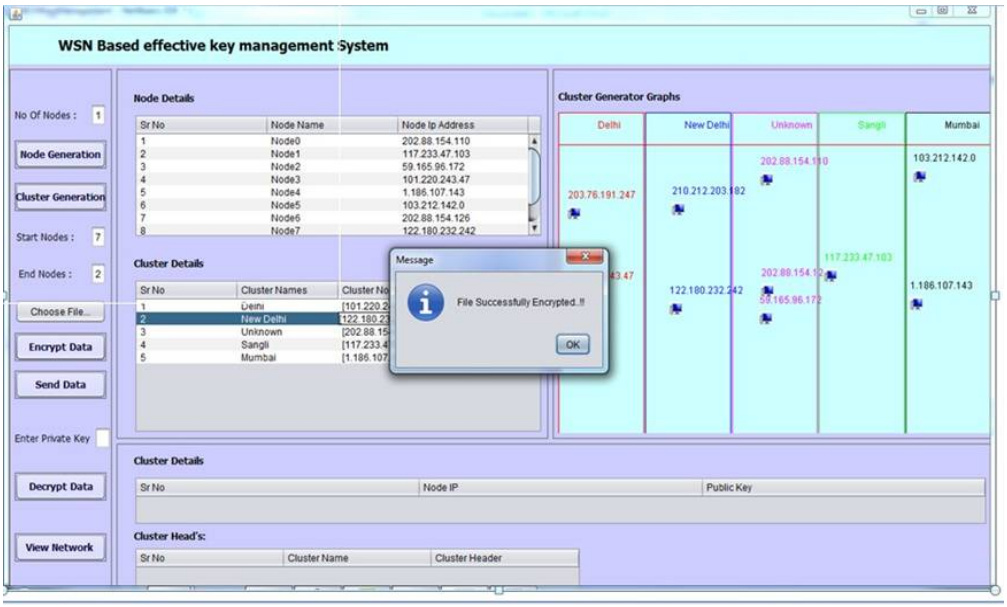
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

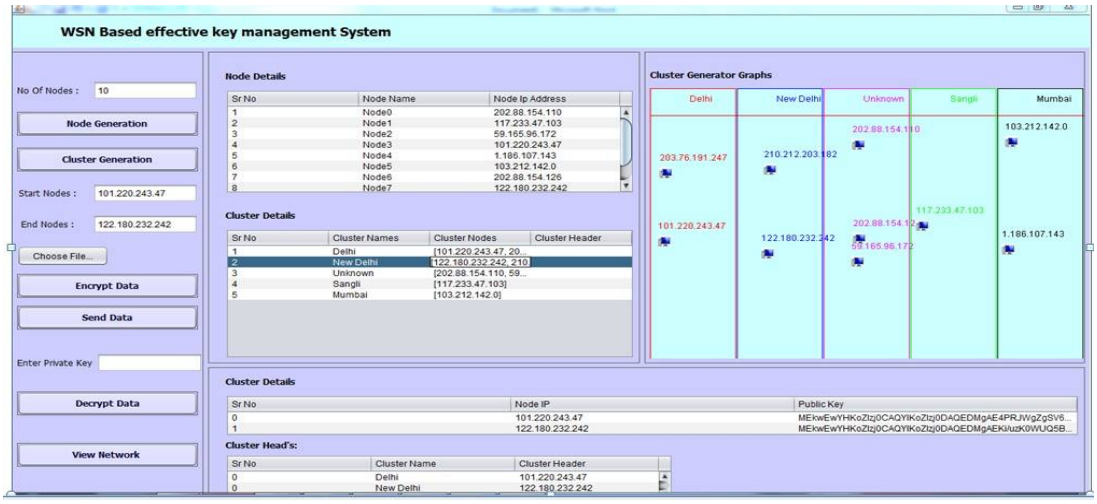
Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018



3. Message sending from source to destination

How packet is send from source to destination with the help of intermediatenodes.Theintermediatenodesarenothingbuttheclusterheadsandthe sensor nodes. The message is Send via shortest path between source and destination.



4. Message decryption

How decryption is done on the destination side. Decryption needs the source's public key and destination private key. After successful decryption the message is received at the destination.

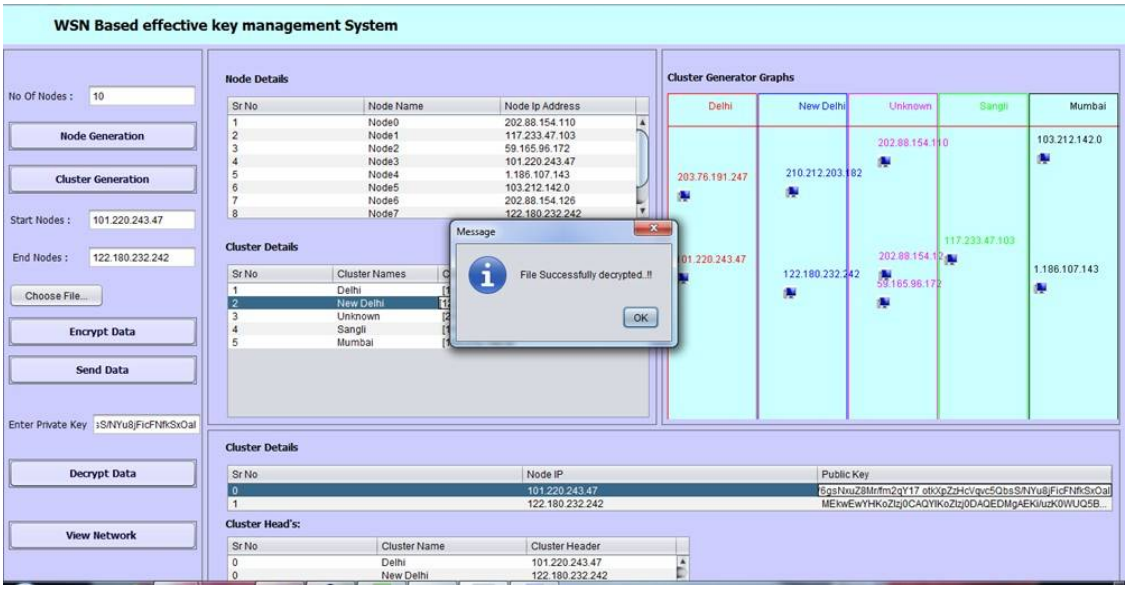
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

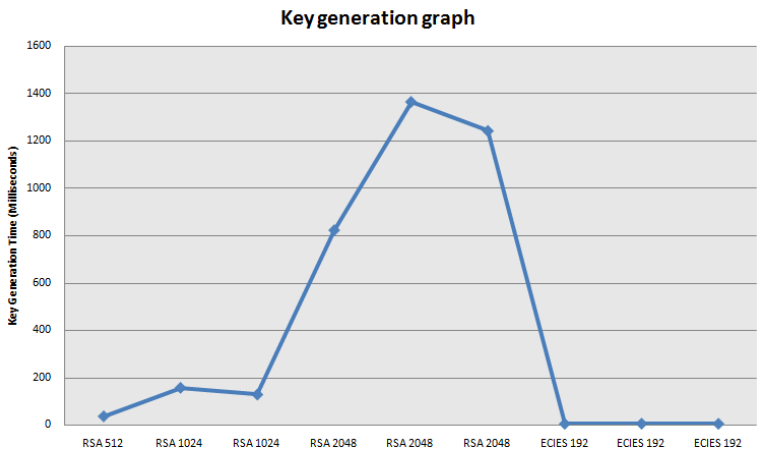


5. Communicationgraph

The communication graph, as we send a message from one node to other node. The source and destination can be in same cluster or in different clusters. So, the communication graph shows how the data is send from cluster head to cluster head if source and destination are in differentclusters.

6. Encryption and decryption timinggraph

The message encryption time, message sending time and message decryption time with respect to number of nodes for 100mb file size.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

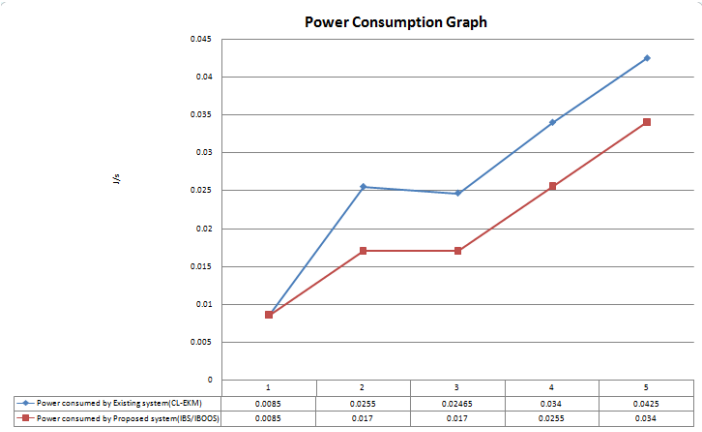
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

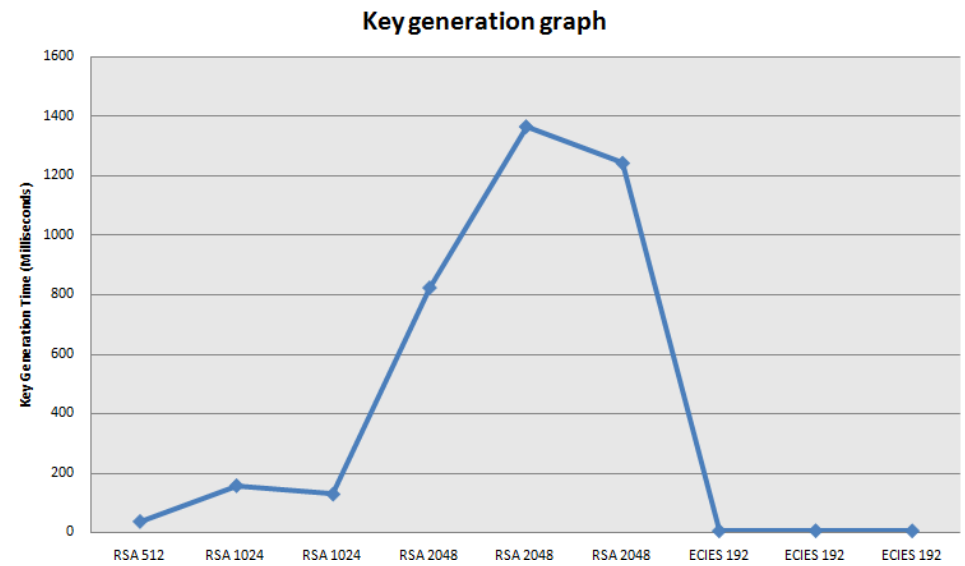
Vol. 7, Issue 5, May 2018

7. Key generationgraph

The key generation time for RSA and ECIES algorithms with differentkeysize.Thekeygenerationtimeiscalculatedinmilliseconds with respectto different key size of algorithms. From this graph we can analyze that which algorithm with how much key size is suitable for our system. The graph shows that RSA-512 need less time than RSA-1024 and RSA-2048. And the ECIES-192



is also need very less key generation time. So from this graph we can conclude that, as key generation time is less it will not spend more energy key generation time and help to improvethe efficiency of proposedsystem.



V. CONCLUSIONS

Through this dissertation, we have addressed effective key management using IBS and IBOOS protocols. IBS and IBOOS protocols are more active than traditional passive techniques.

- Wepresentalgorithmtogeneratethekeysforefficientkeymanagementwhich gives the more security

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

to the data sending over the network.

- We have successfully integrate the IBS and IBOOSapproach.
- Analysis and experiments show the better results as compared with existing system. The main goal of this research is concerning the protocols IBS and IBOOS have better performance than the existing secure protocols for WSN.

ABBREVIATIONS

Abbreviations	Description
WSN	Wireless sensor network
IBS	Identity based digital signature
IBooS	Identity based online and offline digital signature
ECC	Elipticcurvel Cryptography

REFERENCES

1. Seung-Hyun Seo, JonghoWon, Salmin Sultana, "Effective key managment in dynamicwirelesssensornetworks,"inIEEETransactiononInformationforesics and security., vol. 10, No. 2, pp 371-382, Feb.2015.
2. H. Chan, A. Perrig, and D. Song, "Random key predistributionschemesfor sensor networks", in Proc. IEEE Symp. SP, pp. 197-213, May2015.
3. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme forsensornetworksusingdeploymentknowledge",IEEETrans.DependableSe- cure Compute., vol. 3, no. 1, pp. 62-77, Jan./Mar.2014.
4. M.A.MatinandM.M.Islam,"OverviewofwirelesssensornetworK",Journal of Computing Science and Engineering 4 (2012)3361.
5. Hamza Khemissa, Djamel Tandjaoui,2014, "A Novel Lightweight Authentica- tion Scheme for heterogeneous Wireless Sensor Networks in the context of In- ternet of Things", in Proc. 8th Int. Conf.ICISS, vol. 7671, pp. 194-207, April 2012.
6. OsmanYagan,Member,andArmandM.Makowski,Fellow,"WirelessSensor Networks Under the Random Pairwise Key Predistribution Scheme: Can Re- siliencyBeAchievedWithSmallKeyRings",inProc.1stInt.Conf.SecureComm, pp. 277-288, Sep.2012.
7. Amar asheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior ember, "Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile SinkinSensorNetworks",ACMTrans.Inf.Syst.Secur.,vol.8,no.2,pp. 228-258, Feb2012.
8. Manuel Janssen, Andreas Busboom, UdoSchoon, Gerdvon Colln, CarstenKoch, "A Mobile Open Infrastructure Network Protocol (MOIN) for localization andData communication in UWB Based Wireless Sensor Networks", J. Parallel Distrib.Comput., vol. 70, no. 8, pp. 858-870, July 2012.
9. Subir Biswas, MahbubulHaque, Saeed Rashwand, and JelenaMisic,"Fast, Seam- less Rekeying In Wireless Sensor Networks," IET Inf.Secur., vol. 6, no. 4, pp. 271-280, Dec.2011.
10. MumtazQabulio,YasirArfatMalkani,AyazKeerio,"SecuringMobileWireless SensorNetworks(WSNs)againstCloneNodeAttack",inProc.6thInt.WorkshopCryptograph. Hardw.Embedded Syst., pp. 119-132,2011.
11. Daniel Kalus, Michael Muma and Abdelhak M. Zoubir, "Distributed Robust Change Point Detection For Autoregressive Processes With An Application To Distributed Voice Activity Detection," EURASIPJ. Wireless Commun. Netw., vol. 2011, pp. 1-11, Jan.2010.
12. M.S.Albahri, M.Benaissa, "Parallel Comba Multiplication in GF(2163) using Homogenous Multicore Microcontroller", Secur.Commun. Netw., vol. 5, no. 5, pp. 496-507,2009.
13. S. Chattopadhyyay, A. K. Turuk, "A Survey on Key Pre-distribution Scheme in Homogeneous Wireless Sensor Networks", in: Proceedings of the 2nd Inter- national Conference on Advanced Computing and Communication Technologies for high performance Applications,2010.
14. M. A. S. Jr, P. S. L. M. Barreto, C. B. Margi, T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed Wireless Sensor Networks", Computer networks 54 (2010)25912612.
15. R. Manoj, N. Dhinakaran, "A Survey of Key Predistribution Schemes for Key Management in Wireless Sensor Networks", in: Proceedings of the 12th Inter- national Conference on Networking, VLSI and signal processing (ICNVS10), 2010.
16. H. Lee, Y. H. Kim, D. H. Lee, J. Lim, "Classification of Key Management Schemes for Wireless Sensor Networks", in: ASWAN international workshops on Advances in Web and Network Technologies, and Information Management, 2007.
17. S.M.K.R.Raazi,S.Lee,"ASurveyonKeyManagementStrategiesForDiffer- entApplications of Wireless Sensor Networks", Journal of Computing Science and Engineering 4 (2010)235