ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Implementation of Access Control Protocol with Node Privacy in Wireless Sensor Networks Applications

Pooja Patil, N. S. Sirdeshpande, Giridhar. S. Sudi

M.Tech Student, Dept. of ECE, KLS GIT, Belagavi, India

Asst. Professor, Dept. of ECE, KLS GIT, Belagavi, India

Asst. Professor, Dept. of ECE, KLS GIT, Belagavi, India

ABSTRACT*:* Nodes deployed in a sensor network may be lost due to the issues like power exhaustion or malicious attacks. To enhance the lifetime of the sensor network, new node deployment is necessary. In military scenarios, adversaries may directly enter in to the network to capture highly secured activities. In order to control the malicious activities from the adversaries it is necessary to use access control protocol to assure node privacy by the use of authentication techniques and strong encryption algorithms. Our proposed access control protocol concentrate mainly on node privacy using hash function and cryptographic algorithm RSA. How exactly hash function and RSA confirms the authentication and data security among the nodes present in the wireless sensor network is the basic objective of this project. Our access control protocol can defend against most well-recognized attacks in sensor networks, and achieve better computation and communication performance by the use of RSA compared to other algorithms.

KEYWORDS*:* WSN, Hash function, Cryptography, RSA, Access Control protocol etc.

I. INTRODUCTION

Usually in the protocols present today, source node identities are either hashed or encrypted, whereas the destination node identities is been used as plain text, it is not hashed or encrypted. However, in WSN most of the services are generally requested and/or accessed from base stations or gateway nodes. In such scenarios, the concept used above can provide security to source node entirely but it cannot guarantee the security of destination node. Therefore, an attacker easily monitors the activities which are occurring in the network and also can intercept the nodes identity (i.e., destination node). Thus, it is needless to say, the identity privacy of the involved nodes (source to destination and vice-versa) not been properly addressed in real WSNs. RSA and ECC algorithms are the best choices of providing assurance of authentication and privacy.

The aim of this work is to design an access control protocol with node privacy (ACP) that would take care of the node (identity) privacy (i.e., from source to destination and vice-versa) in WSNs. The proposed ACP utilizes RSA, and provides explicit mutual authentication between the (transmitter and receiver) nodes. At the same time, the scheme ensures nodes privacy, i.e., without disclosing their real identities.

II. METHODOLOGY

The proposed system includes the following phases: as depicted in Figure 1.

A. Network Initialization Phase

This phase includes the steps as follows. Generating Fixed Number of Nodes, Clustering the nodes where in K-mean clustering algorithm is used, Electing Master Node Based on the energy values of the nodes in each cluster.

B. Key Management & Authentication Phase

In this phase, Identities of Each node are generated by Master nodes and Circulated to all the others nodes in the respective clusters. Every master node is having the ids of the other master nodes present in the network. Every time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

when any node want to send message the sender node has to verify its destination node identity from master node. This satisfies the Authentication and node security.

C. Communication Phase

Once the authentication is done, the message can be exchanged between the nodes directly. In order to provide security to the message exchange an encryption algorithm is used. The Algorithm used can be RSA.

D. Security Analysis Phase

Where in, we can consider security against the attacks like Forgery, Node Capture, Replay and Interception, finally we can prove that the ACP used here with RSA, Hash Function, Cryptography can provide two level securities as ECC.

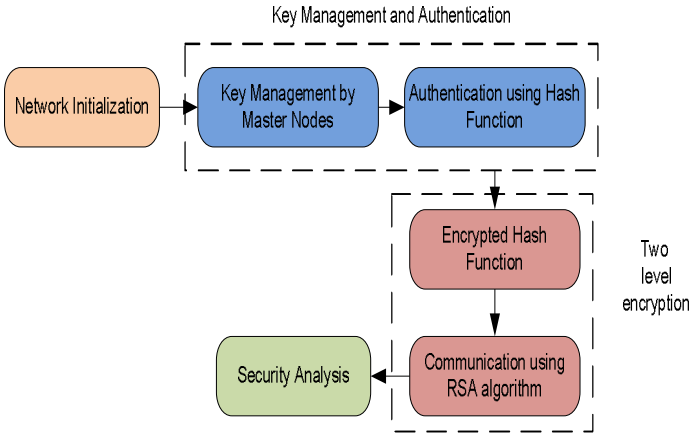

Figure 1: Block Diagram for Proposed System

III. LITERATURE SURVEY

In [1] paper, author investigated the security related issues and challenges in wireless sensor networks to identify malicious activities by using a low power FPGA.

In [2] paper, author discussed the existing Access Control schemes over Wireless Sensor Networks. This paper presents existing Access Control Schemes over Wireless Sensor Networks and discusses how those protocols make safe our Sensor Networks against various types of security threats.

In [3] paper, an identity-based user authentication and access control protocol based on the Identity-Based Signature (IBS) scheme where the ECC (Elliptic Curve Cryptography) based digital signature algorithm (DSA) is used for signing a message and verifying a message for a wireless sensor networks. This protocol accomplishes the registration of a new user, authentication of a user, session key establishment between sensor node and the user; and finally grants the appropriate data access to the user. User revocation is also handled in this proposed protocol.

In [4] paper, author proposed an efficient authentication and access control method based on general view of the security issues for perception layer of Internet of Things (IoT). The advantage of the proposed method is establishing session key based on Elliptic Curve Cryptography (ECC). This enhances mutual authentication between the user and sensor nodes, and intermediate processes. On the other hand, this method solves the resource-constrained problem in perception layer of the Internet of Things.

In paper [5] provided an overview of security threats and attacks, outlines the security requirements and presents a state-of-the-art survey on access control models including a comparison and evaluation based on their characteristics in WSNs. Potential challenging issues for access control schemes in WSNs are also discussed.

In [6] paper, author presented the overall analysis and review of the recent research works along with the proposed architecture of an integrated approach to privacy and security with its simulated results for Access Control in WSNs.

IV. IMPEMENTATION

The Access control protocol follows the following implementation steps as creating network with clusters and master heads, key distribution, authentication and data communication. The detailed explanation of the above steps with flowchart is as given in Figure 2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A. Network Creation

The network is created with user specified number of nodes. Then the cluster formation is done using K-mean clustering method. It forms clusters based on considering cluster centres it again depends upon how many clusters we want to create, the nodes whose distances are nearer to the cluster centres are added to the corresponding clusters.

The table is formed for every cluster by considering their x and y id's, energy, keys and cluster which the node belongs to. Based on the energy level, the node which is having the highest energy is considered as Master Head which is responsible for having hash tables for authentication process of cluster nodes to which it belongs to. Upon the election of Master heads, keys are distributed to all the other nodes in the clusters by their respective Master Heads.

B. Authentication & Data Communication

When any node wants to communicate with any other nodes in the network, it is obvious that for security factor the authentication process has to carry out. The authentication has to be done by the trusted party itself which already has the table of existed number of nodes and their respective keys.

Once the source and destination nodes are specified then source node puts its own id, destination id and its own key in hash and encrypts it with its key and passes it to Master Head to verify whether the destination node is authenticated or not for further data communication. Once master head receives that message it will decrypt it using source nodes key and verifies for the destination node by referring to its hash table. If the destination node exists then it displays it as authenticated. Else it checks for that destination node existence in the other clusters by communicating with other cluster's master heads. If any cluster

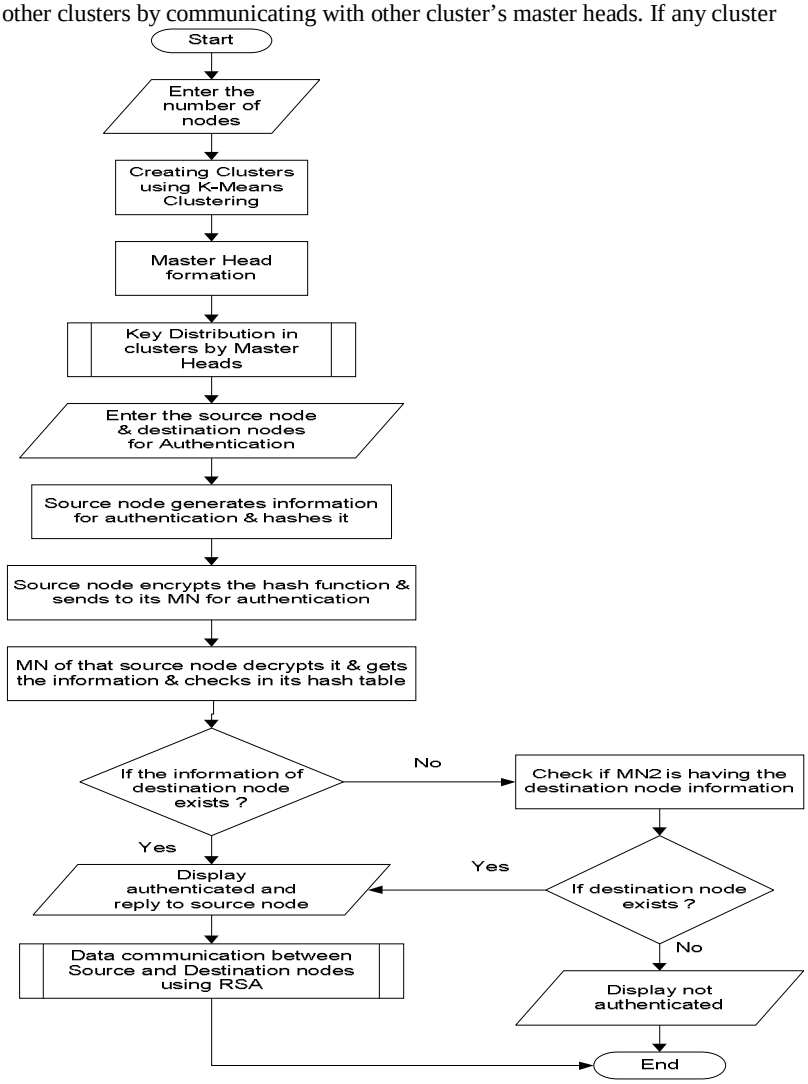

Figure 2: Overall Flow covering all the phases

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

head finds the destination node in its hash table then replies to requested clusters master head. Upon the reception of destination node existence message it acknowledges to source node saying that the node is authenticated. If the destination does not exist in the network then master node displays as unauthenticated.
Once the authentication of the destination node is done then source node can directly send the data to the destination node. But in order to provide security to the data that has to be shared between the source and destination nodes some encryption technique is necessary to be used. The algorithm used here is RSA. First the pair of keys is generated, one is encryption key and another is decryption key. The source node encrypts the data with encryption key and directly passes it to destination node.
The destination node upon receiving this message decrypts it with decryption key and reads the information that has been shared by source node.

V. EXPERIMENTAL RESULTS

A. Network creation with Key Distribution

The following Figure 3 shows the network creation with clusters and master heads. Key distribution from master heads to other nodes in their respective cluster.

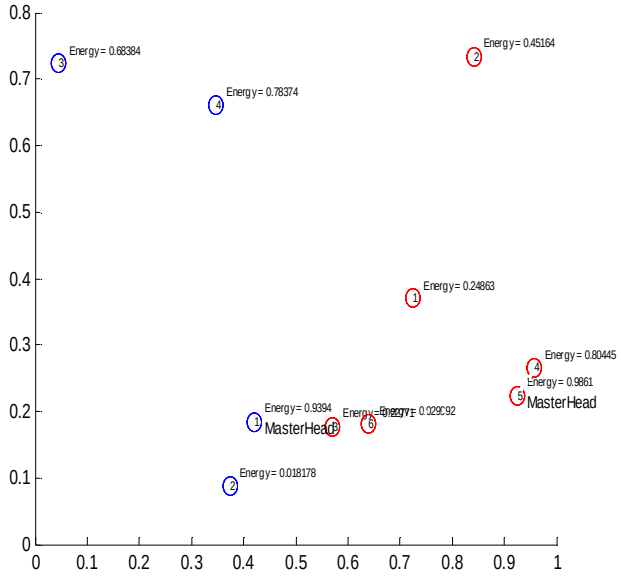

Figure 3: Network Created with Clusters.

B. Authentication & Data Communication

As shown in Figure 4 below for cluster head in one node checks for authentication of source node 2 and destination node 3. It displays that node 3 is not authenticated and passes the hash table to another cluster 2 for authentication. If the node is authenticated then the message is displayed as authenticated so that data can be passed to that node directly.
Data communication is done after the destination node authentication confirmation from master node is received. Sender can readily encrypt the message to be shared with the destination node using RSA encryption algorithm and passes to the authenticated destination node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

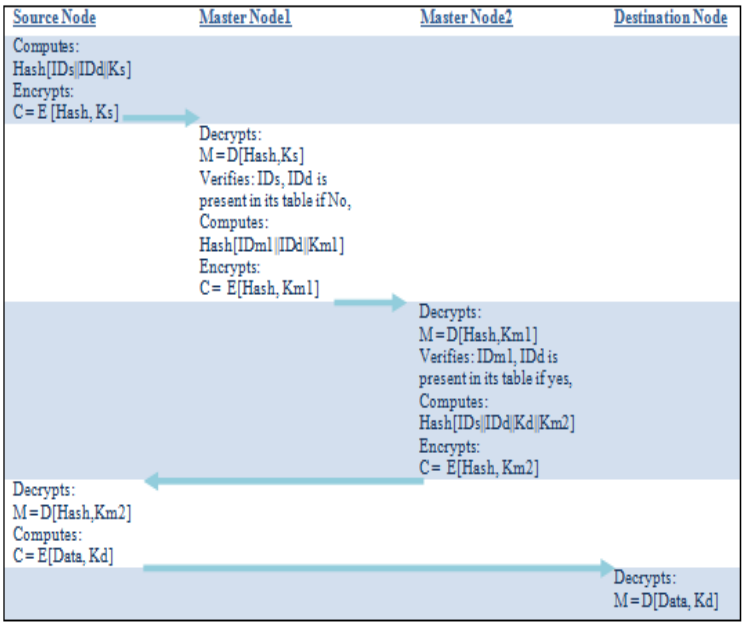

Figure 4.Authentication & data communication phases considering two cluster scenario

Table 1: The Notations used and their Descriptions

Notations Used	Description
M	Message or Data
H( )	Hash Function
IDs	Identity of source Node
IDd	Identity of Destination node
IDm1, IDm2	Identities of Master Head 1 & 2
Ks, Kd	Keys of Source & Destination Node
Km1, Km2	Keys of Master Heads 1 & 2
||	Concatenation sign
E(M,Ks), D(M,Ks)	Encryption & Decryption of Message using Ks

C. Attack Security

When any malicious node enters the network for communication pretending as one among the nodes which are already been identified and their keys are known to the Master nodes in respective clusters as shown in Figure 5. If that malicious node wants to communicate with any node in the network also theauthentication of that node is checked by the master nodes in their respective clusters and if that node is not authenticated by one master node, the authentication has to be checked by the other master nodes present in the network. If the node is not authenticated by any master nodes in the network that node is considered as malicious and further communication with that node is not permitted.
The Table 2, Includes the comparison between the considerations which are used in both existing and proposed methodologies. From the table it is clear that our proposed method provides “Two Level Encryption” as compared to already existed technologies.
Our proposed scheme can also provide the security against the attacks like Replay, Node masquerade, Sybil, Node forgery, Node Capture and Node privacy attacks. The number of communications or processes increases as number of nodes increases by considering normal and attack conditions is plotted in Figure 6.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

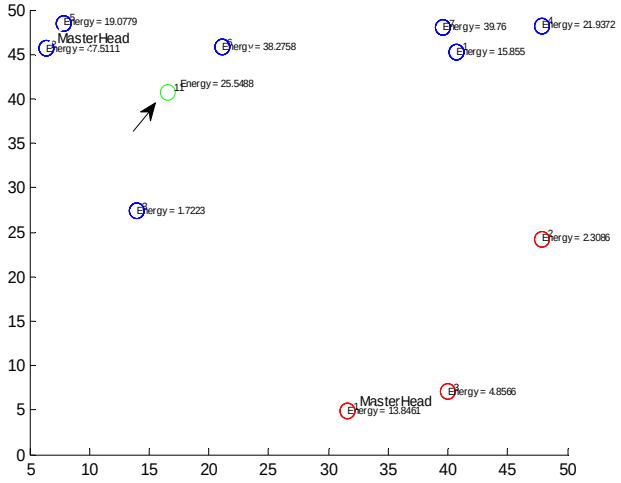

Figure 5: Attack Security considering Attack node

As illustrated in Figure 7 that describes the throughput with respect to attack and normal conditions for N=15. And throughput is defined as the number of successful transmissions with respect to time. Throughput without attack predicts 100% performance compared to under attack conditions. As the number of nodes increases the transmission delay for the communication between the nodes also increases as illustrated in Table 3.

Table 2: Comparison of Existing Vs Proposed Methodology

Considerations	Existing ACP	Proposed ACP
Hash Function	Yes	Yes
Hash Encryption	No	Yes
Data Encryption	Yes	Yes
Data Decryption	Yes	Yes
Attack Security	Yes	Yes

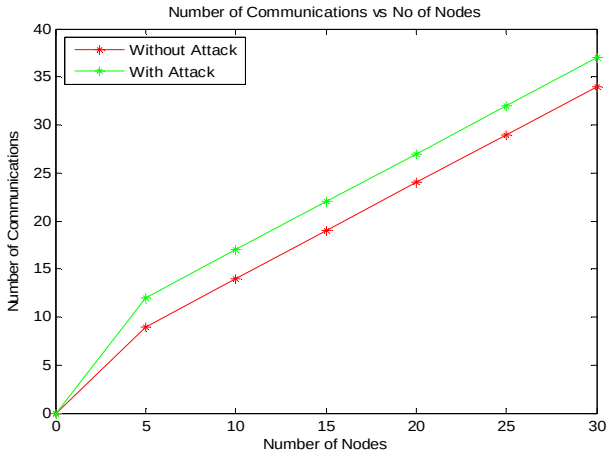

Figure 6: Plot of No. of Communication Vs Number of Nodes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Table 3: Number of Nodes Vs Propagation Delay

Number of Nodes (N)	Transmission Delay (seconds)	
	Within Cluster	Between the Clusters
N = 10	15.20	22.01
N = 15	23.09	29.58
N = 20	30.49	36.98
N = 25	38.19	44.68
N = 30	45.8	52.15

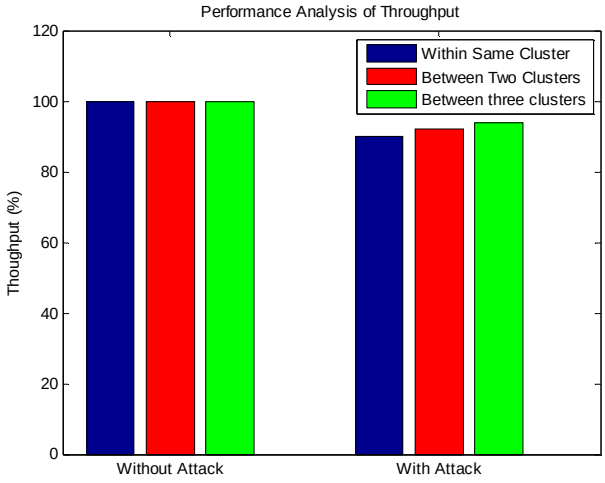

Figure 7: Throughput Vs with normal and attack conditions for N=15

VI. CONCLUSION

Our implementation mainly concentrated on node privacy by the use of RSA, Hash Function and Cryptography. From the implementation results it is clear that our proposed scheme provide two level communication by the use of encryption of Hash function which is been used for authentication purpose. The proposed ACP with Two level encryption gives more accuracy compared to the other algorithms. It also provides equivalent or little more privacy to the nodes as compared to the use of ECC with one level encryption condition.

Our proposed scheme can also provide the security against the attacks like Replay, Node masquerade, Sybil, Node forgery, Node Capture and Node privacy attacks. In the implementation part it is also shown that how the created network provides security against the malicious node entered inside the network. This model achieves 100% throughput under normal condition and under attack 92%. The transmission delay taken for 15 nodes under all conditions will give us 29.99 and 38.15 sec within and between the clusters respectively.

REFERENCES

[1] Indumathi G and Sylvia Sharon D, "Authentication and Secure Data Access Privacy in Wireless Sensor Networks," International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, 2014.

[2] Abdulla Al-Mahmud andMateiCiobanuMorogan, "Identity Based Authentication and Access Control in Wireless Sensor Networks,"International Journal of Computer Applications, Volume 41, Issue 13, 2012.

[3] Ning YE, Yan Zhu, Ru-chuan WANG, Reza Malekianand Lin Qiao-min, "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things," International Journal of Applied Mathematics and Information Sciences, Volume 8, Issue 4, 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

[4] HtooAung Maw, Hannan Xiao, Bruce Christianson and James A. Malcolm, "A Survey of Access Control Models in Wireless Sensor Networks," Journal of Sensor and Actuator Networks, 2014.
[5] S. Mano Shalini, M. Navaneetha and M. Shivakumar, "An Enhanced Privacy Access and Accountable Security Management in Wireless Sensor Networks," South Asian Journal of Engineering and Technology, Volume 2, Issue 17, 2016.
[6] Yun Zhou, Yanchao Zhang, Yuguang Fang, "Access control in wireless sensor networks", Journal Elsevier, Year 2007.
[7] Boniface K. Alese, Sylvester O. Olatunji, Oluwatoyin C. Agbonifo, Aderonke F. Thompson, " A Fine-Grained Data Access Control System in Wireless Sensor Network", Volume 4, Issue 3, Year 2015.
[8] Dona Maria Mani, Nishamol P H, "A Comparison Between RSA And ECC In Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Volume-2, Issue 3, Year – 2013.
[9] Auqib Hamid Lone, Prof. Moin Uddin, "Common Attacks on RSA and its Variants with Possible Countermeasures", International Journal of Emerging Research in Management &Technology, Volume 5, Issue 5, Year 2016.