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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Implementation of Energy Aware Secure Multipath Routing Protocol in Wireless Sensor Network

Madhuri Zawar, Dipali Salunke

Assistant Professor, Dept. of Computer Engineering, GF's GCOE, Jalgaon, North Maharashtra University Jalgaon, Maharashtra, India

Research Scholar, ME Computer, GF's GCOE, Jalgaon, North Maharashtra University Jalgaon, Maharashtra, India

ABSTRACT: Secure data transmission is major issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Proposed a CRP increases the system performance in effective way .CRP uses digital signature (DSI) scheme for security. In DSI security relies on the DSA algorithm. To improve the performance of the system energy aware Rule based scheme is proposed. Rule-based learning automata increase the network life time. Simulation results shows that proposed system has better performance compared with the existing system in terms of security, efficiency, energy consumption.

KEYWORDS: Cluster Based Wireless Sensor Network (CWSNs), Digital Signature (DSI), Cryptography, Rule-Based Learning Automata.

I. INTRODUCTION

The wireless sensor networks are often used to monitor a remote environment. There are thousand numbers of sensor nodes that works together to monitor the environment (temperature, noise levels, humidity, pressure). These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to one or more collection points [1]. These sensor nodes are connected via wireless media. The sensor nodes are small and expensive. Working such a complex network requires scalable and management technique. Scalability in wireless sensor networks can be achieved by the clustering technique where the numbers of nodes are grouped into various clusters. These networks often use self organizing clustering protocols to form clusters and to establish better communication. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs. Recent studies and researches in WSNs, addressing routing aware techniques, and security solutions are much more interested in CWSNs. These are the major problem in WSNs.

In this paper we have presented design and implementation of energy aware secure routing protocol that provides security and optimal path to data transmission in network. In section I wee have given the introduction of wireless sensor networks, problems related to the wireless sensor networks. Section II discusses the existing system with their drawback and objective of proposed protocol. Section III describes the DSA algorithm with digital signature scheme in details.the section 4 discusses the implementation of the proposed protocol with its phases. In Section V ,we have simulated all the secure and routing protocols and also shows the result of protocol.wee have analysed how the proposed protocol provides better security and multipath routing to network.

II. LITERATURE SURVEY

There is a number of cluster based routing and security protocol currently used in the field of network security situation awareness, such as LEACH [2] and Sec-LEACH [2]. They achieves improvements in terms of network lifetime and security of the information The SET-IBS and SET-IBOOS protocols in [3] are implemented by using ID based digital signature and ID based online/offline digital signature. The SET-IBS protocol is implemented for the security in network by using the ID based digital signature. The orphan node problem is solved by the SET-IBS protocol. The SET-IBOOS Protocol is implemented for also security and reducing the computational overhead of storage. The scalability of network is high. It means number of nodes can work in network. The offline signature

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

scheme is not suitable in the CWSN. The offline signature is computed by third party. These protocols are using the symmetric key management technique of cryptography. In that technique the Third party can be access the packet through the public key. It harms to the communication between nodes.

By using these protocols, the data can be transmitted in secure and efficient way into the network. The Routing mechanism provides the better path for routing packets and the network lifetime is improved. They lack the capability of analyzing and assessing other security related information such as vulnerabilities and threats. Also they are not able to solve the problems of selection path for routing the packets in networks.

A. *Protocol Objective*

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between nodes, as well as transmission between CHs and the BS [3]. It his paper, we aim to implement the digital signature using RSA algorithm which uses asymmetric key management for providing the better security. The learning automata are used for saving the energy of node and help to improve the network lifetime. The digital signature scheme is used to authenticate to the receiver.

III. DSA ALGORITHM

A. DSA - Digital Signature Algorithm:

The DSA algorithm in [4] is used with digital signature to implement the asymmetric key management.

1) Key generation:

Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

2) Parameter generation:

- Choose an approved cryptographic hash function H. In the DSS, H is always 2.
- Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). Choose an N-bit prime q. N must be less than or equal to the hash output length.
- Choose an L-bit prime modulus p such that $p–1$ is a multiple of q.
- Choose g, a number whose multiplicative order modulo p is q. The value of g is calculated by using eq.(1)

$$g = h^{(p-1)/q} \bmod p \qquad \text{eq.(1)}$$

for some arbitrary h $(1 < h < p-1)$. Most choices of h will lead to a usable g; commonly $h=2$ is used.

- The algorithm parameters (p, q, g) may be shared between different users of the system.

3) Per-user keys:

Given a set of parameters, the second phase computes private and public keys for a single user:

- Choose x by some random method, where $0 < x < q$.
- Calculate y

$$y = g^x \bmod p \qquad \text{eq(2)}$$

Public key is (p, q, g, y). Private key is (p, q, g, x).

There exist efficient algorithms for computing the modular exponentiations $h^{(p-1)/q} \bmod p$ and $g^x \bmod p$, such as exponentiation by squaring.

4) Signing:

Let the hashing function and m the message: Generate H be a random per-message value k where $0 < k < q$

- Calculate r by using eq.(3) .

$$(y = g^k \bmod p) \bmod q \qquad \text{eq.(3)}$$

- Calculate s by using eq.(4) .

$$s = k^{-1}(H(m) + xr) \bmod q \qquad \text{eq.(4)}$$

5) The signature is *(r,s)x*Verification :

- Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
- Calculate w using eq.(5).

$$w = s^{-1} \bmod q \qquad \text{eq.(5)}$$

- Calculate $u1$ using eq.(6).

$$u1 = H(m).w \bmod q \qquad \text{eq.(6)}$$

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

- Calculate *u2* using eq.(6).
  $$u2 = r.w \ mod \ q$$
- Calculate *v* using eq.(7).
  $$v = \left((g^{u1} y^{u2}) mod \ p\right) mod \ q \qquad \text{eq.(7)}$$
- The signature is valid if $v = r$. Authentication is done.

B. Learning Automata:

Sensors are redundantly deployed, a subset of sensors should be selected to actively monitor the field (referred to as a "cover"), while the rest of the sensors should be put to sleep to conserve their batteries [5]. Despite of its potential application, wireless sensor network encounters resource restrictions such as low computational power, reduced bandwidth and specially limited power resource. In this paper we are implemented learning automata based for energy-efficient monitoring in wireless sensor networks.

Learning Automata are used for choosing the nodes having redundant coverage contribution. The method in comparison to existing methods uses many numbers of nodes for monitoring network area.

IV. PROPOSED PROTOCOL

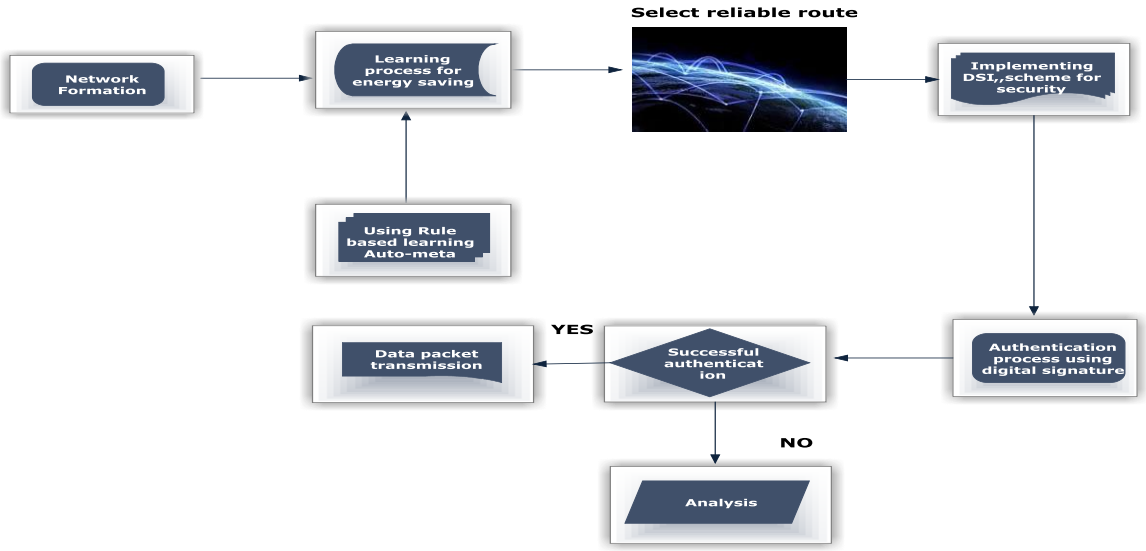

Fig.1.Flow Diagram of Protocol

A. *Phases*

The fig. 1 shows the diagrammatical representation of the protocol with its sequence.

1) Network Formation:

Networks are formed with the given range of the sensors. Nodes are grouped into cluster automatically depends upon their radio waves. Agents are formed for group registration.

2) Learning Phase:

Learning automata is a machine that can do finite actions. Each selected action is evaluated by a possibility environment. Evaluation results are given to automata through positive and negative signals and automata uses these results to choose the next action. The ultimate goal is that automata can learn to choose the best among all. Here variable structure learning automata algorithm is used for select the reliable and optimum route.

3) Update Routing Phase:

Each node has learning automata with action number equal to number of paths from that node to destination. The protocol uses this to select appropriate path in order to balance energy usage.

4) DSI scheme Implementation Phase:

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

The proposed system implements two Secure and efficient data transmission protocols for CWSNs, called DSI and DSOO respectively. The key idea of DSI is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocol, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem.

5) Data transmission Phase:

The Proposed system uses the Homomorphism encryption for encrypting the data packet and uses hash functions for identifying the varying length and digital signature scheme for authentication. If the authentication is successful then it sends data packet through the Reliable routing path.

6) Analysis:

Various aspects of data transmission in wireless sensors are analysed .In Learning Phase, rule based learning is analysed for selecting reliable route and its performance metric is compared with the existing system. Proposed a new protocol scheme DSI is also analysed for security metrics. Finally comparative analysis is made for security, energy-efficiency, and performance.

V. RESULT AND ANALYSIS

The simulation studies involve the wireless network with 61 nodes as shown in Fig.1. The proposed secure energy aware protocol is implemented with Network simulator. We transmitted data packets through source node 8 to destination node 35. The node 8 selects the path for routing the packets and after discovering the next intermediate node it forwards the packet to the next node. The node selects the route using learning automata. According to that packet delivered to the proper destination. At destination side, the authentication process is performed to get access of the packet. For the authentication purpose digital signature is used. Proposed protocol is compared with energy, performance, network lifetime, bandwidth throughput.

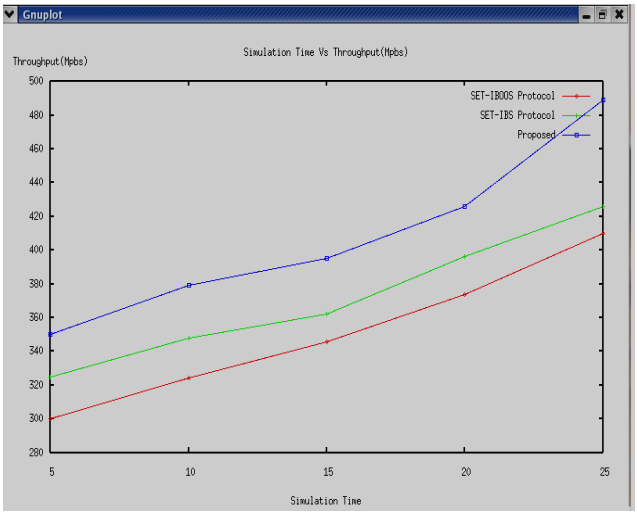

Fig. 2. Simulation Time Vs Throughput

In fig. 2 shows the simulation time vs throughput. The simulation time is start into simulator that time is increase the throughput and showing the existing system and proposed work comparison. Simulation time is nothing but starting and ending times. The throughput indicates the successfully sent the no of packets from source to destination. The proposed protocol sent the more no of packets into the network in few milliseconds. So, the throughput of proposed protocol is more than the other protocols.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

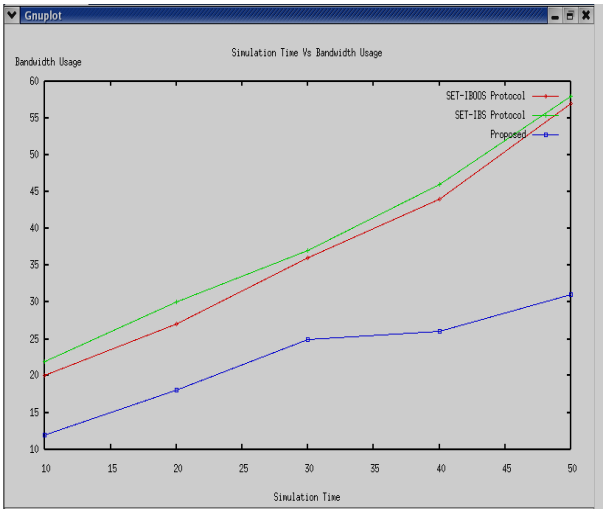

Fig. 3. Simulation Time Vs Bandwidth

In fig. 3 shows the simulation time vs bandwidth. The proposed protocol took less bandwidth compare to existing model. In proposed protocol its take less bandwidth for sending packets because packets are encrypted. In less bandwidth, the proposed model sends maximum packets without loss or drop packets. The other protocol requires more bandwidth for transferring the packets from source to destination.

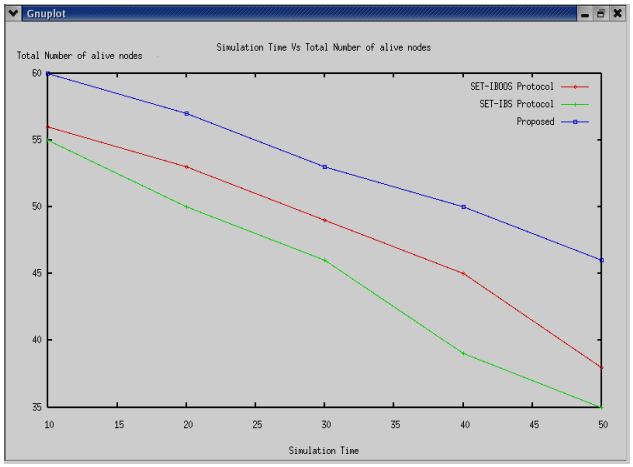

Fig. 4. Simulation Time Vs Number of Alive Nodes

Figure 4 shows the simulation time vs. number of alive nodes. The number of alive nodes graph shows the increased ratio that mean number of node are alive for long time into the network. The proposed protocol is energy efficient protocols. Because of this,the performance of the network is increased.Proposed protocol improves the network lifetime with the help of learning automata that selects the best node for routing the packets. As compared other routing protocols, there are more number of nodes alive in network.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

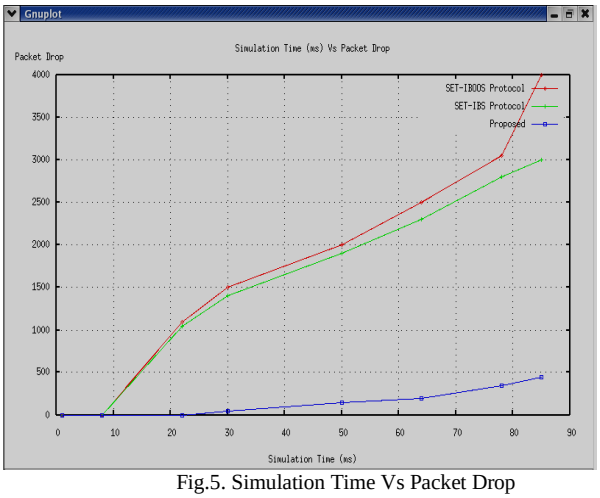

Fig.5. Simulation Time Vs Packet Drop

In fig. 5 shows the simulation time vs. packet drop. Packets could not drop because of the learning automata; it selected the best optimal path of high energy nodes. Nodes having the less power are not used in the packet transmission so the packet dropping is less. In proposed protocol dropped only 1 or 2 percent of packets. The packets ratio is very less. In the other protocols, packet can be dropped because of intermediate node failure, the less energy of intermediate node. So, There packets can be lost into the network. Sometimes it fails to give acknowledge to source.

VI. CONCLUSION AND FUTURE WORK

In this paper we present secure energy with multipath routing protocol for WSNs. The protocol achieves the more security by applying hashing technique and digital signature algorithm. Digital signature use asymmetric key of cryptography. The hashing technique and DSA algorithm used for authentication. The learning automata are applied to select the best optional path for routing for data packets in a network. It improves the life time of network by saving the power of nodes. Finally comparative analysis made for security, energy-efficiency, and performance. Simulation result is showing energy aware, secured data transmission with high level performance using this protocol.

ACKNOWLEDGMENT

I would like to thank Mrs.Madhuri Zawar Professor of Computer Department for valuable time, guidance and suggestions during the hour of paper. I accord my sincerest gratitude and profound thankfulness, for his insistent guidance, insightful opinion and constructive comments. I would like to express my special gratitude and thanks also HOD of Computer Department Prof. Dipak R. Pardhi other staff members for giving me such attention and time.

REFERENCES

[1] Hara, V.I. Zadorozhny, and E. Buchmann, "*Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence"*, vol. 278. Springer-Verlag, 2010.

[2] A.A. Abbasi and M. Younis, "*A Survey on Clustering Algorithms for Wireless Sensor Networks*," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841 , 2007.

[3] Huang Lu, Jie Li, Mohsen Guizani,*"Secure and EfficientData Transmission for Cluster-Based Wireless Sensor Networks*",IEEE Computer Security,vol. 25, no. 3,pp. 750-761, 2014.

[4] Hongwei Si, Youlin Cai,, Zhimei Cheng," *An Improved RSA Signature Algorithm based on Complex Numeric Operation"*, IEEE Computer Security,pp.399-400,2010.

[5] Jalil Jabari Lotfa, Mehran Hosseinzadehb,seyed hossein hosseini nazhad ghazanic,Rasim M. Alguliev "*Applications of learning automata in wireless sensor networks"*, Elsevier,Procedia Technology 1,pp. 77 – 84,2012.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

BIOGRAPHY

Mrs. Madhuri R. Zawar received the B.E and M.E. Degrees in Computer Science and Engineering from Dr. Babasaheb Ambedkar Marathwada University, Maharashtra, India, in 1996 and 2011 respectively. Since 2007, she has been with the GF's Godavari College of Engineering, Jalgaon, NMU University, where she is currently an Assistant Professor of Computer Engineering. Her research interests include Wireless adhoc Networking. In these areas, she has presented a paper in iCOST 2011 International Conference, Dhule and presented a paper in absence at IEEE ICCSIT 2011 International Conference, China. She has a membership of ISTE. She has published paper in IJECSCSE 2015journal.

Ms. Dipali A. Salunke received the B.E Degree in Computer Engineering from North Maharashtra University Jalgaon, Maharashtra, India, in 2010. Currently, she is studied in ME Computer Engineering in North Maharashtra University,Jalgaon. Since Aug. 2010, she has been with the G.H.Raisoni Polytechnic, Jalgaon, where she is currently Lecturer of Computer Engineering. Her research interests include Wireless Networking. In these areas, she has presented a paper in ICACSIT 2012 International Conference, Pune, Maharashtra. She has published paper in IJECSCSE journal 2015.