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

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st&22ndMarch Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Distributed energy efficient Secured routing For Wireless sensor networks

S.MathuMitha, S.KaviPriya, T.Revathi

PG Scholar, Dept of Computer and Communication, Mepco Schlenk Engineering College, Sivakasi, TamilNadu, India.

Assistant professor, Dept of Information technology, Mepco Schlenk Engineering College, Sivakasi, TamilNadu, India.

Head of the Department, Dept of Information technology, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India.

Abstract-Routing is aprocess of determinin ga path between source and destination upon request of data transmission. A secured Routing is typically required to avoid the attack occurred in routing. The sensor operates on the battery power it is very important to make efficient use of energy for sensor to increase the lifetime of the network. Distributed energy efficient secured routing for wireless sensor network will deal with both security and energy of the wireless sensor network. Security is provided by evaluating the trust value for each and every node in sensor network and also the energy is also evaluated for each and every node to find the neighbor node for securely routing the information. Existing System deal with the cryptographic technique to provide the security in routing hence attacks are not avoided Proposed system deal with both the security and energy
Of the wireless sensor network, hence the attacks occurred are reduced.

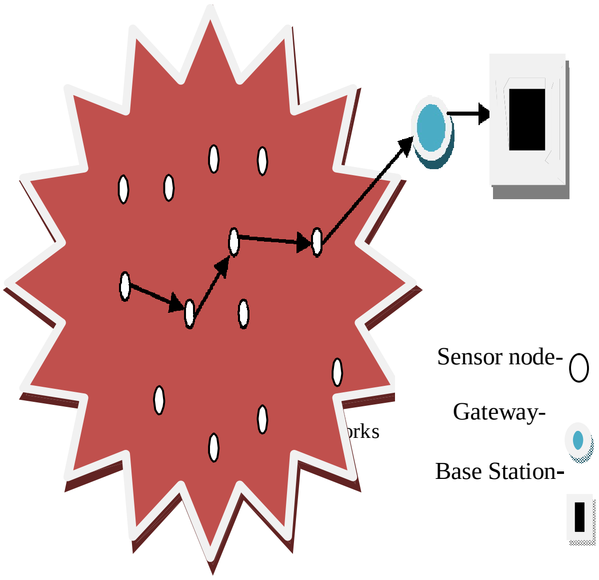
Keywords -Cryptographic Technique,Secured Routing,Wireless Sensor Networks.

I.INTRODUCTION

Wireless sensor network consists of collection of senso rnode arranged in the specific manner. Sensor node senses the environment or event and report data to base station. Multi-hop routing in WSN will transmit packets to multiple wireless links to reach the base station(Fig 1).

Malicious attacks will occur in multi-hop routing in WSN hence security must need to be provided for WSN. An adversary node will implementan attack like wormhole in sensor network .An attacking node that colludes with the valid node and receives routing packets and replay to the node that is faraway from original node is wormhole attack [1]. Several other attack slike selective forwarding, Sybil attack, sinkhole attack[2] also occurred inrouting due to identity deception.

Sensor nodes contain less amount ofenergy hence energy mustneedtobe utilizedinanefficientmanner in WSN. To utilizeenergyinefficientwayenergy watcherisused. Thesecuritymustneedto be provided inroutinghence,the data delivered to the base station is highly secured.Toprovidethesecurity inrouting trust managerisintroduced thatavoid the routing of packets through the attacker node.



Existing Protocol in WSN provide honest and energy efficiency in nodes [3] authentication for packets provided by encrypting data using this adversary can be eliminated. TinySec [4], Spins [5], TinyPK [6], and TinyECC [7] these are some of examples for authentication schemes in WSN.

II.AUTHENTICATION REQIREMENTS

Distributed energy efficient secured routing for WSN use asymmetric authentication of broadcast packet from the base station. Guarantee need to provide that adversary node will not forge a packet from the base station. Distributed energy efficient secured routing for WSN also use the trust manager to select a trustworthy path for transmission in the presence of attacker node.Asymmetric authentication is used because in symmetric authentication the adversary can enter in to the network illegally using a key.Examples of asymmetricauthenticated broadcast schemes are in [8], [9].

I. GOAL

Distributed energy efficient secured routing for wireless sensor network is mainly protected against attacks occurred in WSN and it will not deal with the Denial-of-Service Attack [10]. Distributed energy efficient secured routing for wireless sensor network provides the following goals.

A. High Throughput

Distributed energy efficient secured routing for WSN throughput is one of the main goal. To achieve the high throughput WSN must need to collect and deliver the data in an efficient way. Retransmission and duplicate packets also consider as one packet so packets need to be utilized in efficient way to achieve the higher throughput.

B. Energy Efficiency

Distributed energy efficient secured routing for WSN provide energy efficient by hop-per-delivery here the energy is measured using one-hop node transmission. Due to lot of energy consumption using retransmission hop-per-delivery is considered to achieve energy efficiency.

C. Scalability & Adaptability

Distributed energy efficient secured routing for WSN work for large scale WSN in a dynamic manner, hence scalability goal also need to achieve.

II. ROUTING METHODOLOGIES

Wireless sensor networks contain several routing techniques. Here a periodic service routing protocol is used where the routing information is exchanged and updated for a particular length of that period. First base station broad cast information about data delivery in last period.Broadcast message is asymmetrically authenticated so guarantee will be provided that adversary node not forges message. Second energy report delivered to the neighbor node after receiving broadcast message from the base station. Energy watcher receives energy report from neighbor,and then records the energy value for neighbor node in neighborhood table. The compromised node may falsely report that it requires a low energy cost to deliver the packet so that compromised node selected for the next hop node. To avoid such adversary node trust value is calculated for each node with the help of trust manager. Trust manager will maintain the trust level entries for neighbor node. These energy and trust values maintained in neighborhood table for each and every node.

III. ENERGY WATCHER

Energy watcher is responsible for calculating the energy value for a neighbor node from energy report send by the neighbor node these energy values are entered in neighborhood table. Consider ‘N’ as the node ‘E_N’ is an energy cost for node ‘N’. Energy watcher is responsible to calculate the energy value for node ‘N’ and computed value is ‘E_{Nb}’ is energy cost required to deliver unit sized data to the base station is entered in neighborhood table with ‘b’ as the next hop node it is responsible for remaining route.

$$\mathbf{E_{Nb}=E_{N\text{->}b}+E_b(1)}$$

Where $E_{N\text{->}b}$ is the average energy cost of successfully delivering a data packet form ‘N’ to its neighbor ‘b’ as one hop node. E_b is energy cost broadcast form one hop node ‘b’ to ‘N’. To calculate the average number of one hop sending before an acknowledgement is received.

$$\mathbf{p_{succ}.(1-p_{succ})^{i-1}=1/p_{succ.} \qquad (2)}$$

The probability of successfully delivering packet is represented as p_{succ}.

Now E_{Nb} is calculated to generate one-hop transmission after acknowledgement

$$\mathbf{E_{Nb}=E_{unit}/p_{succ}+E_b(3)}$$

Here E_{Nb} is calculated for remaining job and get probability p_{succ} that one hop transmission is acknowledged.

In wireless sensor node they use weighted averaging technique to calculate p_{succ} using weighted averaging technique p_{new_succ} is calculated using p_{old_succ} , *Ack*is updated by 1 acknowledgement is received otherwise 0 and two different weights $w_{degrade}$ (0,1) will assign high value if fault and the high risk is occurring .

$$\mathbf{p_{new\_succ}=(1-w_{degrade})*p_{old\_succ}+w_{degrade}*\mathit{Ack}\text{ if }\mathit{Ack}=0(4)}$$

$w_{upgrade}$ (0,1) assign a low value if the positive transaction can’t provide good connectivity and need many more positive transactions.

$$\mathbf{p_{new\_succ}=(1\ -w_{upgrade})*p_{old\_succ}+w_{upgrade}*\mathit{Ack}\text{ if }\mathit{Ack}=1(5)}$$

IV. TRUST MANAGER

The trust manager assign 0.5 as default value for all neighbor nodes and detect loop occurred in network or not is identified by whether packet received is already present in the table or not if it present trust manager degrades its next-hop node's trust level and record the loop value as 0 .

$$T_{new\_Nb}=(1-w_{degrade})*T_{old\_Nb}+w_{degrade}*loop \text{ if } loop=0 \quad (6)$$

A packet received is not present in the table, then trust value will be upgraded and assign loop values as 1.

$$T_{new\_Nb}=(1-w_{upgrade})*T_{old\_Nb}+w_{upgrade}*loop \text{ if } loop=1(7)$$

Trust manager also calculates trust value of the neighbor node based on*Delivery Ratio* which is calculated from a broadcast message from the base station. *Delivery Ratio* is less than T_{old_Nb} then trust value will be degraded.

$$T_{new\_Nb}=(1-w_{degrade})*T_{old\_Nb}+w_{degrade}*\text{Delivery Ratio if Delivery Ratio}< T_{old\_Nb}(8)$$

If the delivery ratio is greater than or equal to the T_{old_Nb} trust value will be upgraded.

$$T_{new\_Nb}=(1-w_{upgrade})*T_{old\_Nb}+w_{upgrade}*\text{Delivery Ratio if Delivery Ratio}>= T_{old\_Nb}(9)$$

V. ANALYSIS ON ENERGY WATCHER AND TRUST MANAGER

Energy Watcher and Trust Manager are used to select the optimal neighbor node as next-hop neighbor node. Trust manager will not recommend to another trust manager about trust value. The trust manager identifies the optimal route to transmit data without any attacker node and defeat the intention of attacking node and calculate trust value based on the broadcast message from the base station. The trust manager finds out many delivery failures from broadcast message trust manager degrade trust value if the trust value goes below a threshold level then node take alternate next-hop node.

Fig 2 is an example for work of trust manager. It contains five nodes (A-B-C-D-E) with one attacker (E) node and base station. Node A chooses the path A-B-E-Base station transmits packet to base station. Base station broadcast message in regular interval. Nodes A receive broadcast messages from the base station in the path Base station-D-C-A. Analyzing the message node A concluding that attacker node present in the path A-B-E hence node A choose alternate path A-C-D-Base station.

Node A also alters the trust value for B as very low. Even though B is not the attacker node. The routing path of B contains attacker node hence A will select trust routing path and increase the trust value for node C.

Fig 3 is an example for working of trust manager and energy watcher. It contain nodes (1-2-3-a-b-c-d-Base station) routing path selected for base station is (a-b-c-d) here node (a-b-c) contain table with the trust value and energy cost for neighbor node.

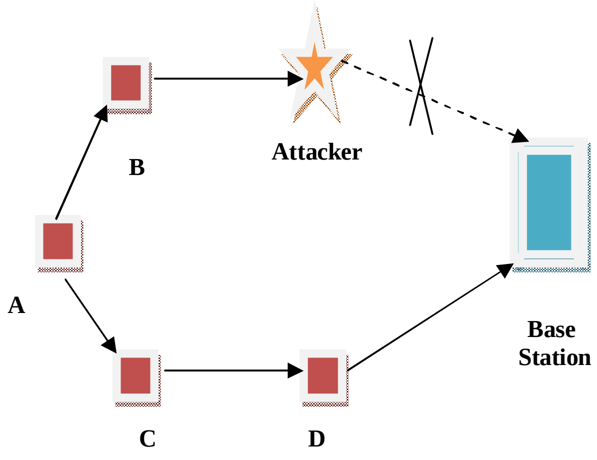


Fig 2: Example for Trust Manager Work.

Node 'a' contain neighbor node 1,2,b with energy (E_{a1},E_{a2},E_{a3}) and trust value (T_{a1},T_{a2},T_{a3}) respectively. Comparing neighbor trust and energy value node 'a' select 'b' as neighbor node.

Node 'b' contain neighbor node 3, c with energy (E_{b3},E_{bc}) and trust value (T_{b3},T_{bc}) respectively. Comparing neighbor trust and energy value node 'b' select 'c' as neighbor node.

Node 'c' contain neighbor node 3,d with energy (E_{c3},E_{cd}) and trust value (T_{c3},T_{cd}) respectively. Comparing neighbor trust and energy value node 'c' select'd' as neighbor node.

Node'd' is one hop node to base station node'd' deliver packet to base station. The routing path is (a-b-c-d-base station).

Distributed energy efficient secured routing for WSN will select the trustworthy route with the help of trust watcher and also consume energy by energy watcher. Authentication of packets provided with the help of asymmetric key authentication.

Distributed energy efficient secured routing for WSN is designed to protect against the attacks occurred in WSN. Trust Manager also protects from the attack caused by injecting packets to produce wrong route.

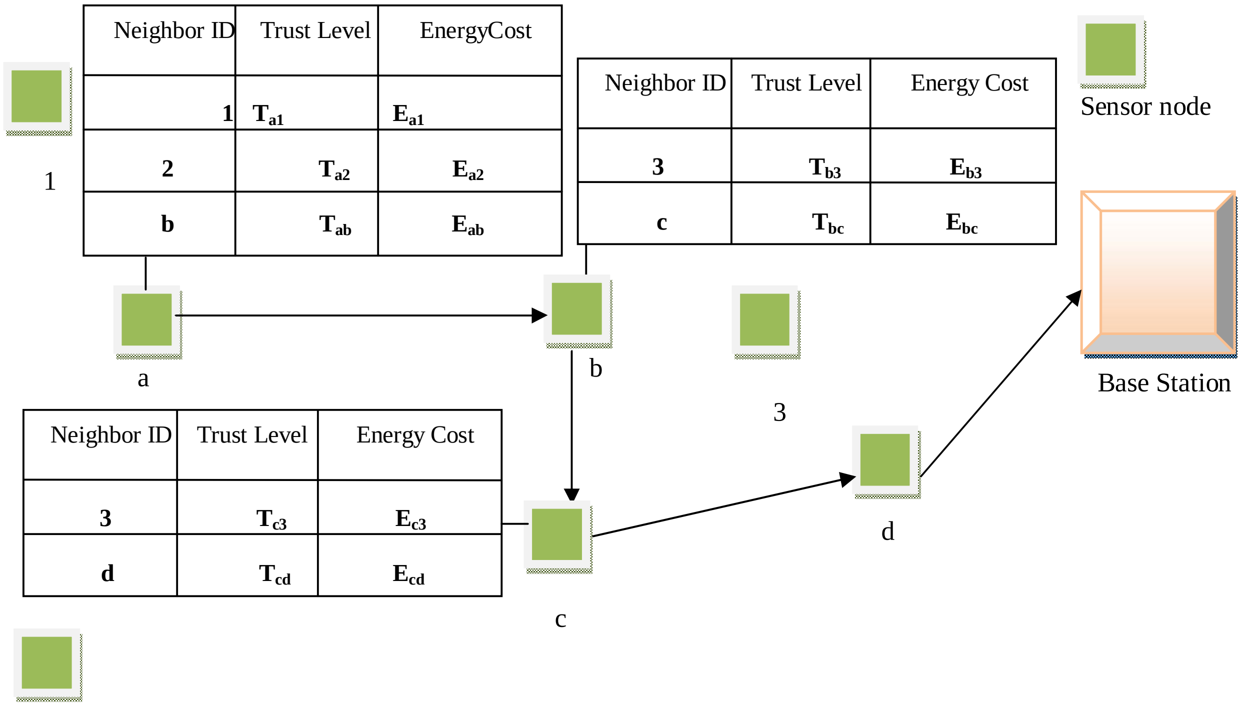
Distributed energy efficient secured routing for WSN will not require any tight time synchronization and also about geographical routing.

VI. SIMULATION AND IMPLEMENTATION

The Distributed Energy Efficient Secured Routing for WSN is simulated using Network Simulator - (NS2). Sensor Nodes are deployed in equally spaced manner. Grid Topology is used to deploy the sensor node in WSN.

Fig 4 contain 25(0-24) nodes are deployed and consider Node '4' as source node and Node '24' as Base Station.

In fig 5 Node '9' and Node '14' are consider as attacker node hence source Node '4' will calculate the trust value for node neighbor node after calculating the trust value it decide that Node '9' is attacker node and take alternate path (3-8-13-18-23-24).

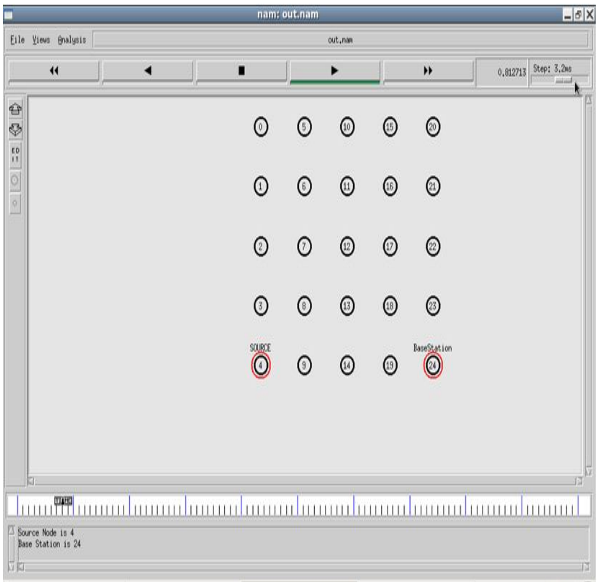


Neighbor ID	Trust Level	EnergyCost
1	T_{a1}	E_{a1}
2	T_{a2}	E_{a2}
b	T_{ab}	E_{ab}

Neighbor ID	Trust Level	Energy Cost
3	T_{b3}	E_{b3}
c	T_{bc}	E_{bc}

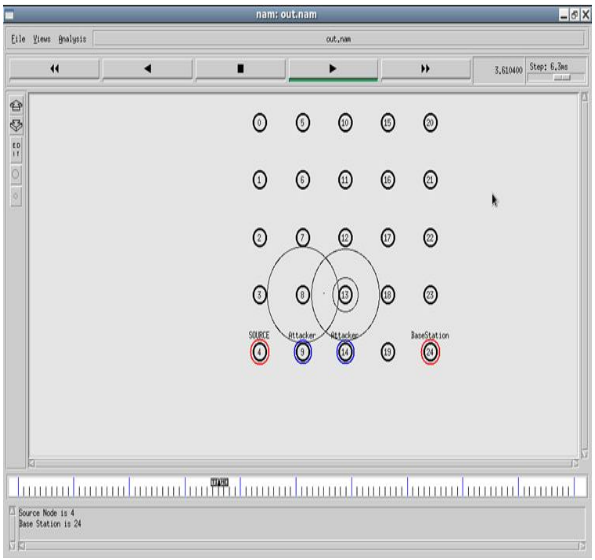
Neighbor ID	Trust Level	Energy Cost
3	T_{c3}	E_{c3}
d	T_{cd}	E_{cd}

Fig 3: Working of Trust Manager and Energy Watcher.



```
Source Node is 4
Base Station is 24
```

Fig 4: Grid Topology



```
Source Node is 4
Base Station is 24
```

Fig 5: Routing Path Selection after calculation of Trust and Energy Value.

VII. Conclusion

Distributed energy efficient secured routing for wireless sensor network implemented energy efficiency using energy watcher hence energy in sensor network is used in efficient way optimal route and optimal neighbor is selected using trust manager so, data packet will reach the base station without any attacker. Distributed energy efficient secured routing for wireless sensor node provides both energy efficiency and security in wireless sensor network and also reduces attacks on sensor networks.

REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, “Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs,” Proc. Seventh European Conf. Wireless Sensor Networks (EWSN ’10), 2010.

[2] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. First IEEE Int’l Workshop Sensor Network Protocols and Applications, 2003.

[3] J. Al-Karaki and A. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” Wireless Comm., vol. 11, no. 6, pp. 6-28, Dec. 2004.

[4] C. Karlof, N. Sastry, and D. Wagner, “Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks,” Proc. ACM Int’l Conf. Embedded Networked Sensor Systems (SenSys ’04), Nov. 2004.

[5] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, “SPINS: Security Protocols for Sensor Networks,” Wireless Networks J., vol. 8, no. 5, pp. 521-534, Sept. 2002.

[6] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “Tinypk: Securing Sensor Networks with Public Key Technology,” Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN ’04), pp. 59-64, 2004.

[7] A. Liu and P. Ning, “Tinyecc: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks,” Proc. Seventh Int’l Conf. Information Processing in Sensor Networks (IPSN ’08), pp. 245-256, 2008.

[8] S.Chang, S. Shieh, W. Lin, and C. Hsieh, “An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS ’06), pp. 311-320, 2006.

[9] K.Ren,W.Lou,K.Zeng, and P.Moran,“On Broadcast Authentication in Wireless Sensor Networks,”IEEE Trans. Wireless Comm.,vol.6,no.11,pp.4136-4144,Nov.2007.

[10] A.Wood and J.Stankovic,“Denial of Service in Sensor Networks,”Computer,vol.35,no.10,pp.54-62,Oct.2002.