Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Energy Efficient Routing in Wireless Sensor Network-A Survey on Existing Techniques

Reshma Patil*, Prof.Sharmila.M.Shinde
Computer Engineering Dept.
Pune University, India

Abstract— Wireless Sensor Network are special kind of Ad-hoc networks. There are number of application for wireless sensor networks like military, healthcare and civil areas and security is important for many of them. However WSN suffers from many constraints like low computation capability, small memory, limited energy resources, lack of infrastructure which impose security challenge. Traditional security mechanism is not suitable in WSN. Security in WSN is challenging task. This paper discuss need of security, security requirements, various type of attacks, we also discuss existing security techniques like cryptography, Steiner based security mechanism, Trust based security mechanism, a minimum hop routing techniques for home security and discuss some future direction for research.

Keywords— Wireless Sensor Networks, energy efficient, security, security mechanisms.

I. INTRODUCTION

A] Introduction to WSN:

A wireless sensor network is collection of thousands of tiny wireless sensor nodes for data communication purpose. These sensor nodes cooperate with each other to accomplish data transmission. A variety of wireless sensor networks have been developed for different applications like military, healthcare, civil, bridge monitoring, home automation in the recent years. Sensors are inexpensive, low power devices, which have limited resources.

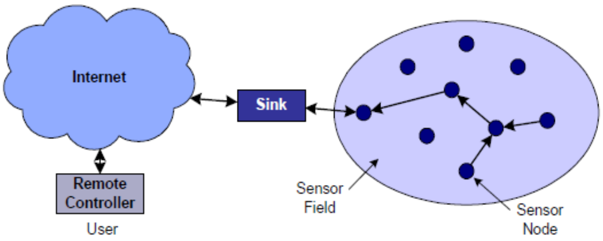

Figure 1. WSN Architecture

Figure 1 shows system architecture of wireless sensor network. It contains collection of sensor node. Each node contains a power unit, a processing units, a storage units, sensing unit and wireless transmitter/receiver The Sensor nodes communicate with each other wireless to transmit data from one node to another node. Number of applications is built in WSN. Cost of sensor node depends on complexity of applications .The sensors are still available at low cost. Generally star topology is used in WSN, but it may depend upon external parameters to mesh or some other topology.

B] Introduction to Energy Efficiency:

There are different constraints present in WSN like energy constraints, memory limitation, unreliable communication, higher latency in communication. So energy consumption is very important constraint in WSN. There are several reasons we will discuss later one by one. Basically lifetime of sensor networks entirely depends on battery power of sensor nodes. Battery power supplies the energy needed by device to performed task. Actually battery power is limited budget that is the reason we required energy consumption. Whenever node is in active mode energy required, suppose any task performed by sensor node that should be in minimum energy that is nothing but energy consumption.

C] Need of Security:

Routing plays an important role in security of WSN. At the time of design of routing protocol security issue into consideration. Sensor nodes are not enough defences so node can easily capture. Attacker node can easily listen and modify the data on channels. Routing protocol exchange information between the nodes. There is need to establish route between source to destination and transmit that information through air so any attacker hacks that information and sends incorrect information to destination node. Network layer of Wireless Sensor Network is highly insecure and unreliable. There are various security issues in network layer of WSN.

D] Security Challenges:

Open architecture of WSN is biggest challenge of security. Defence against attacker is difficult task in Wireless Sensor nodes. Nodes in WSN are unattended environment.WSN nodes deployed randomly in environment. Major challenge for employing any efficient security scheme in WSN is created by the size of sensors, the processing power, limited memory and type of task expected by the sensors. Battery power limitation is another challenge.

E] Energy Efficient Secure Routing:

Routing protocol routes the data from source to destination. We already discuss what is mean by energy efficiency. So Energy efficient secure routing means we routes packet from source to destination in minimum energy with considering security as an extra parameter.

F] Security threats and attacks:

Most of the threats and attacks in WSN are similar to the traditional network. Due to broadcasting nature of WSN it is more vulnerable. There are different types of attack[2] against the WSN.

- *Denial Of Service:*

The DOS attack tries to busy the available resource by the victim node by sending extra unnecessary packets result is other network users can't uses the available resources. DOS attacks not only disrupt or destroy the network but also block the services. Prevention from the DOS attack requires strong authentication and identification of traffic.

- *Attack on information in transit:*

The information during transit may be altered, spoofed, replayed again. This node provides wrong information to sink node.

- *Sybil attack:*

In WSN Sensor nodes are works together for complete any task. Sensor nodes divide their task into subtasks and redundancy of information. In this condition node can represent to be more than one node is known as Sybil attack.

- Blackhole attack:

This type of attack a malicious node represent as black hole to attract all the traffic in the sensor network. Once malicious node inserts into the network. Then it able to do anything with packet passing between them.

- *Wormhole attack:*

Wormhole attack is one of the critical attacks. In this type of attack attacker records the packet at one location and tunnel those to another location. In this attack no need to compromising a sensor node.

G] Security requirements:

WSNs are special kind of Ad-hoc networks. Security services in WSNs are needed to protect the information and resources from attacks. Security requirements in WSNs include availability, authorization, privacy, authentication anonymity, resilience, confidentiality**,** integrity and Flexibility. There are different security techniques available in WSN. We are going to discuss some available security mechanisms and their limitations in detail.

II. EXISTING SECURITY TECHNIQUE IN WIRELESS SENSOR NETWORKS

There are different security techniques available in WSN. We are going to discuss some available security mechanisms and their limitations in detail.

1. *Cryptography Techniques:*

In cryptography techniques[2] contains encryption and decryption methods. Traditional network uses cryptography technique for security purpose. Cryptography contains different techniques for security like symmetric cryptography, asymmetric cryptography. Cryptography techniques mostly used in wired networks. Cryptography techniques are not to be applied directly on wireless sensor network. WSN contains tiny sensor nodes which contain small memory, limited power battery and lack of processing. These are the limitations of the sensor nodes. Whenever applying any encryption scheme that requires extra energy, extra processing time and these are the important resources for sensor nods. In WSN applying encryption the result is increasing delay, jitter and packet loss.

Another major problem is how to manage keys. How the keys will be modified time to time for encryption.

Disadvantage:

1. Cryptography not suitable for WSN.
2. Required large processing time, memory and energy.
3. Key management is very difficult in WSN.

2. *Steiner Based Security Techniques:*

Steiner Based multicast routing protocol[1] includes control on energy consumption as well as security requirements. SHSMRP protocol combines the concept of Steiner tree and cluster network topology result is scalable and energy efficient for large group communication in WSN. Secure data communication includes data integrity, security and verifiability. RONG fan proposed Steiner based secure multicast routing protocol in two parts.1.Multicast routing protocol based on Steiner tree.2.Secure multicast protocol.

1st protocol integrates Steiner tree and hierarchical network topology in single framework. So this integration allows to be optimized energy efficiency reducing the overhead.

2nd protocol adapts secure communication mechanism to ensure data integrity, security and verifiability.

We assume that each node get its position information accurately by some location service like GPS or other for their network uses basic geographical routing protocol.

Consider WSN Network is a graph V(G,E),G=Set of vertices that is network node. E=Communication link between the nodes.(a,b) € E, a is able to communicate with b neighbourhood set defines as,

N(a)={B € G \ b ≠ a ∧ (a ,b) € E}

Node state information table shown in figure 2.Every node maintain its own state information table.

PID	DID	ClusterHead Flag	Height Value	Membership Flag	Father Node
Node23	(23,49)	1	2	1	(13,33)

Figure 2. Node state information table.

A] Steiner based hierarchical multicast routing protocol:

Steiner based hierarchical multicast routing protocol contains five phases.

1. Node information gathering phase:

In this phase for joining network requires every node should get location information by any some location service after that send join message to source node S that message also include location information. Source node collect location information of all node and store into the database and next step prepare building Steiner tree.

2. Steiner tree construction phase:

Steiner tree construction begins with source node it uses cluster network topology for building Steiner tree. One node added to Steiner tree it set as cluster head, Source node S marks other ungrouped node as its member node .It follows some steps:

1. Initialize each node’s node state information table.
2. Source node S set itself cluster head height value set to 0.
3. Source node S marks nodes inside its radio range as its MN and exclude these node from process of Steiner tree.

Initially S is cluster node n1,n2, n3set as member node then source node search for nearest ungrouped node. In figure next ungrouped node is an n6 and mark other nodes n12,n13 as MN of n6 create logical link between n6 and source node S logical hop distance between source node S and n6 is 1.Collection of source node and node n6 searches for next ungrouped node again this procedure apply for all nodes.

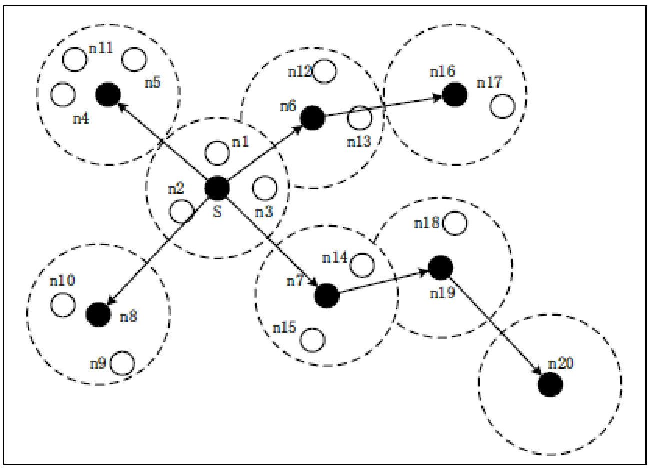

Figure 3 Shows Steiner tree constructions

Steiner tree divided into subtree for improve efficiency of multicast receiver identification is include in multicast packet due to limit number of receivers in one multicast packet.

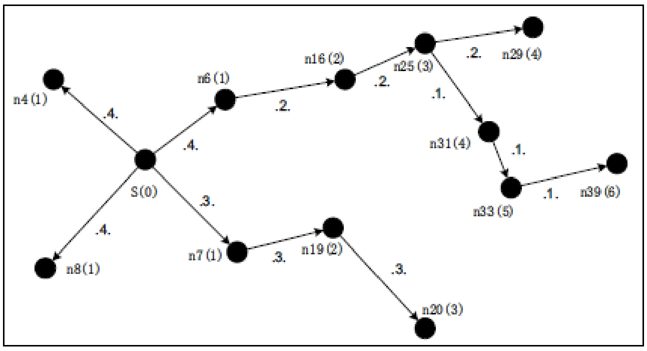

Figure 4 Removes MN

In figure 4 shows removes MN from figure 1 in bracket represent height value of every node..

3. Steiner Subtree distribution phase:

Steiner tree divide into subtree after that source node broadcast topology structure to all subtree. Each node receives topology message if any node detect that message comes itself then it is CH otherwise set as MN. And join the cluster by JOIN cluster message distance from CH and MN it should be less than CH radius of radio range it is easy for MNs to JOIN the cluster.

4. Data Delivery phase:

In this scheme sensing data in WSN in done by using geographical information it is meaningless. If source node wants to send data is determines region of multicasting then source node selects the related subtree which is geographical scope from local database Steiner tree consider as unit source node sends data to a root node of subtree CH forwards the packet according to CH height value if destination detects destination then it broadcast the content of multicast packet.

5. Steiner tree maintain phase

If new node wants to join the multicast group it should obtain the location information and send the join multicast message to source node. If CH sends JOIN SUBTREE message to any subtree then that tree can join cluster.

B] Steiner based hierarchical secure multicast routing protocol:

Logical key hierarchical structure is used for Steiner based hierarchical secure multicast routing protocol.Figure 5 shows logical key hierarchy.

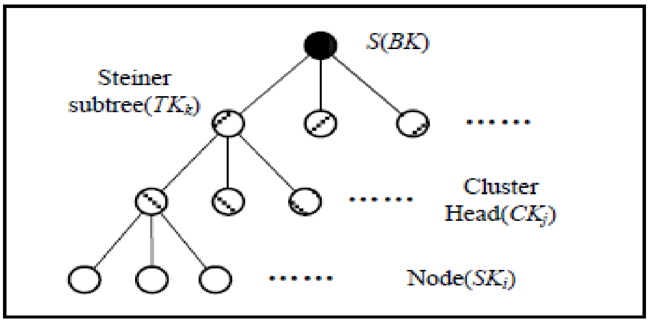

Figure 5.Logical Key Hierarchy

1. Verifying of each node because malicious node will not be join the network. Authentication of each node is take place in this phase.

$$n_i \to S : PID_i, DID_i, T, HMAC(SK_i, PID_i \,||\, DID_i \,||\, T)$$

2. In this phase calculate HMAC value and hash values compare those values for integrity and authentication purpose. Calculate in following steps.

$$\text{Calculate } M_s = E(SK_i, BK \,||\, TK_k \,||\, CK_j)$$

$$M_h = HMAC(SK_i, DID_i \| M_{n_i} \| M_s \| T)$$

3. This phase is data delivery phase. Source node transmit multicast packets as unicast.

$$S \rightarrow * : HEAD, E(TK_k, M), T,$$
$$HMAC(TK_k, HEAD \| E(TK_k, M) \| T)$$

Then, each *CH* who is the destination of multicasting broadcasts the content of multicast packet by this formula

$$CH_j \rightarrow n^* : E(CK_j, M), T, HMAC(CK_j, E(CK_j, M) \| T)$$

In this phase check time stamp value and HMAC value. If the inequality| *Clock* □*T* |<Δt holds and computing result is equal to *HMAC* in the received message, *MNs* accept the content of multicast packet.

4. In this phase rekeying for each node in the network. Specially for temporary session key to rekey the expired key.

$$S \rightarrow n_i : DID_i, E(TSK_i, M_{K'} \| K'), T,$$
$$HMAC(TSK_i, DID_i \| E(TSK_i, M_{K'} \| K') \| T)$$

Advantages

- It provides data security. By using HMAC function data integrity, data secrecy, authentication is maintained.
- Attacker can't launch impersonal attack.
- Attacker can't launch wormhole attack and Sybil attack.

Disadvantage:

- More energy requires.
- It is not applicable in network topology maintain and establish redundant links.

2. *Trust Based Security Schema:*

In general we can say security and trust are highly coupled and can't separate each other. In trusted schema key exchange is not happens without requisite security service is placed. Trust is the expectation of one entity about the action of another.

A] Trust aware routing protocol:

In Figure 6 shows trust management schema [4] it contains monitoring component, trust management component, direct interaction trust table, indirect trust table, trust evaluation component, trust decision component. Together it works as trust management.

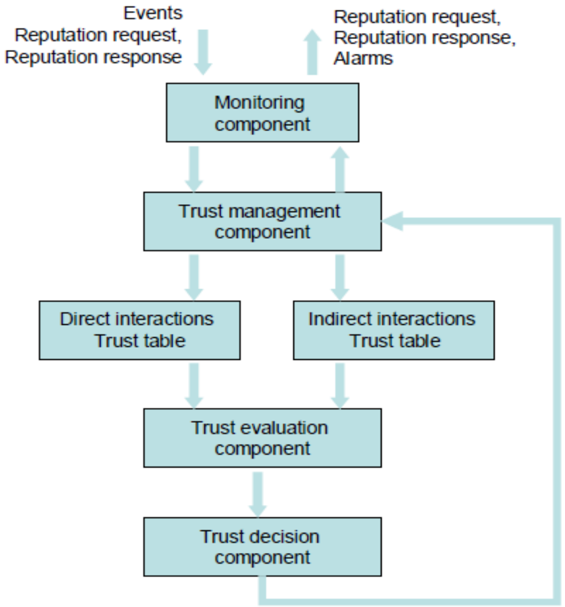

Figure 6. Trust management Scheme

There are mainly two types of interaction trust.

1. Direct interaction trust

2. Indirect interaction trust.

The main objective of trust management scheme is defence against wide set of attacks by monitoring multiple behaviour aspect shown in Table 1.

Table 1: List of trust metrics

Nr.	Trust metric
1	Forwarding
2	Network-ACK
3	Data integrity
4	Node authentication
5	Data confidentiality
6	Reputation Responses
7	Reputation Validation
8	Remaining Energy

Different trust metrics are available like forwarding, network –ACK, data integrity, node authentication node confidentiality**,** reputation, responses, reputation, validation, remaining Energy. This all allows for better load balancing and higher protection against attacks. Trust cost function combines trust energy and location information for guide decisions. Three control message are used namely BEACON, REPREQ and REPRES, last two requires to support reputation schema for indirect trust information exchange with nodes. The quantification of trust for each monitor behavior listed in table1.

The node(i)calculates a trust value related a neighboring node (j) consider trust metrics (m)by dividing the number of successfully completed interaction to be the total number of attempted interaction.

$$T_m^{i,j} = \frac{S_m^{i,j}}{S_m^{i,j} + F_m^{i,j}} \qquad (1)$$

Insert formula 1

The trust values calculated for the monitored behaviors are combined in a weighted sum to produce the direct trust value:

$$DT^{i,j} = \sum_{1}^{7} (W_m * T_m^{i,j}) \qquad (2)$$

The number of received (*k*) reputation responses (REPRES) is summed up in a weighted manner with the weight representing the relevant trustworthiness (*Np*) of the node that provided it:

$$IT^{i,j} = \frac{\sum_{p}^{k} \left(DT^{i,Np} * DT^{Np,j} \right)}{\sum_{p}^{k} DT^{i,Np}} \qquad (3)$$

Finally, the Total Trust value of a node (*i*) for a neighbour (*j*) is calculated by combining direct and indirect trust values in the following formula:

$$TT^{i,j} = C^{i,j} * DT^{i,j} + (1 - C^{i,j}) * IT^{i,j} \qquad (4)$$

where *C i* , *j* is the confidence factor which increases with the number of performed interactions. Total trust value in the Routing Function:

$$RF^{i,j} = W_d * T_d^{i,j} + W_t * TT^{i,j} \qquad (5)$$

Where *Wd* and *Wt* represent the significance of distance and trust criterion, respectively, Trust-aware routing protocol specially designed, the efficiency in detecting and avoiding malicious nodes detecting for different types of attacks, different penetration of malicious nodes, different network density and Different weighting factor are considered.

Advantages:

- Trusted communication take places between the sensor nodes.

Disadvantage:

- Increase the energy ratio which is caused by the exchange and processing of the reputation and request message.

4. A Minimum Hop Routing Technique:

Home security [3] is an application of A minimum hop routing technique. This data routing protocol [3] specially designed for a wireless home security network. Life of such a network depends entirely on the lifetime of the battery power, in this routing protocol, protocol select as metrics parameters hop counts and battery power levels. Purpose is to conserve energy as possible in both computations and data communications. Consider the situation some nodes fails or run out of battery then network will not interrupt and find the alternative path.

Shao-Shan Chiang presents an energy-efficient, reliable and robust routing algorithm for wireless sensor networks. In this approach flood the packet for establishing the routing table for every node in the network this is take place before actual data transmission. Routing table contains parameters like child, parent, sibling node with identification and energy level within one hop distance. Now every node having routing table based on that find best next hop node, which has highest energy level to forward the message.

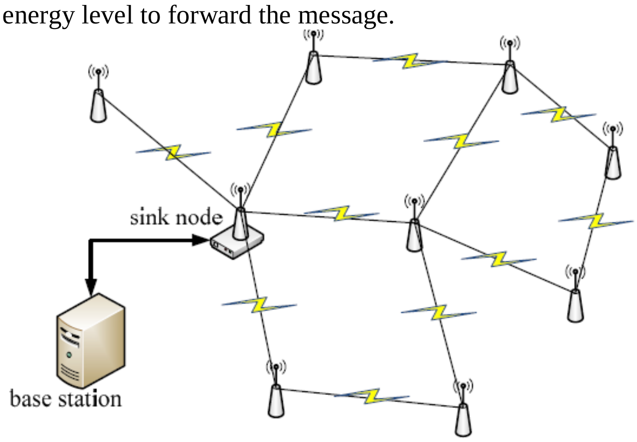

Figure 7. The System model

Figure 7 shows system model it contains base station, sink node and number of WSN nodes. Base station can be located in any space in the house. Sink node is specially designed with more memory compare to other nodes. Sink node connected to base station via wire or wireless links. A sensor node randomly deployed in the house and covers the radio range. During the communication sink node takes commands from the base station and floods the packet to the sensors nodes. A sensor node also collects the data from other sensor nodes and passes to the base station .Except sink node all nodes are battery powered.

There are two phases are used one is routing table establishment and second is data routing phase. In 1st phase flooding technique is used to establish routing table. In 2nd phase routing table remains unchanged until any node failure occurs or a new node is added. Once routing table built data packets to the destination.

Finally Shao-Shan Chiang presented an energy-efficient routing scheme for the wireless sensor network used in home security systems.

Advantages:

- System is reliable and robust.
- Quickly adapt change by updating the routing table and resending packet via new path.

Disadvantages

- Energy consumption is very low.

Here we discuss existing security mechanism in the wireless sensor node. In past researches have design various energy efficient schema for routing in WSN but they did not consider effect of security precautions on cost of energy spending during routing. Here we propose routing schema that consider cost of providing security and its effect of energy efficiency. Security cost contains cryptography cost, monitoring cost and processing cost and which is time based. How much time required for cryptography, monitoring and processing. Minimum energy in term of minimum time required for providing security.

III. CONCLUSION

In this paper, we discussed about the security in sensor networks, security need and attacks in wireless sensor networks. Security is an important requirement and complicates enough to set up in different domains of WSN. The challenges of Wireless Sensor Networks are also briefly discussed. We also discussed available security mechanisms and its strength and limitations. We discussed existing techniques like cryptography, Steiner based security techniques, trust based security techniques, a minimum hop routing technique. We proposed schema that consider cost of providing security and its effect on energy efficiency. Proposed a system which contains security as well as energy efficient parameters.

REFERENCES

[1] Rong Fan, Jian Chen, Jian-Qing Fu, Ling-Di Ping" A *Steiner-Based Secure Multicast Routing Protocol for Wireless Sensor Network*" 978-0-7695-3940-9/10 $26.00 © 2010 IEEE DOI 10.1109/ICFN.2010.50

[2] Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong" *Security in Wireless Sensor Networks: Issues and Challenges"* ISBN 89-551 1044 - Feb. 20-22, 2006 ICACT2006

[3] Shao-Shan Chiang, , Chih-Hung Huang, and Kuang-Chiung *Chang "A Minimum Hop Routing Protocol for Home Security Systems Using Wireless Sensor Networks"* IEEE Transactions on Consumer Electronics, Vol. 53, No. 4, NOVEMBER 200

[4] Theodore Zahariadis "*Implementing a Trust-Aware Routing Protocol in Wireless Sensor Nodes"* 978-0-7695-4160-0/10 $26.00 © 2010 IEEE DOI 10.1109/DeSE.2010.15

[5] Shao-Shan Chiang, , Chih-Hung Huang, and Kuang-Chiung Chang "*A Minimum Hop Routing Protocol for Home Security Systems Using Wireless Sensor Networks*," IEEE Transactions on Consumer Electronics, Vol. 53, No. 4, NOVEMBER 2007.

[6] Tao Shu, Marwan Krunz, and Sisi Liu Department of Electrical and Computer Engineering University of Arizona," *Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes."*

[7] Huei-Wen Ferng,Rachmarini, D. "A secure routing protocol for wireless sensor networks with consideration of energy efficiency"Network Operations and Management Symposium (NOMS), 2012 IEEE .

[8] Siba K. Udgata, "*Wireless Sensor Network Security model using Zero Knowledge Protocol"* IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings.

[9] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, and Michael Chai" *The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks*" IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013.

[10] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados," *Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey*" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.