www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue -9 September, 2014 Page No. 8250-8255

Security Aspects in WSN: Survey and Analysis

***Swati Kakran*[1], *Sunil Kumar*[2]**

[1]Student,A.B.E.S Engineering college
Under Uttar Pradesh Technical University, NH-24, Ghaziabad.
swatikakran@gmail.com

[2]Assistant Professor, A.B.E.S Engineering college
Under Uttar Pradesh Technical University, NH-24, Ghaziabad
Sunil.kumar@abes.ac.in

Abstract: ***In the field of networks wireless sensor network consists of small, large number of sensing nodes which is having the sensing, computational and transmission power. But due to insecure nature of wireless communication, these networks are vulnerable to internal and external attacks. Moreover, routing protocols are designed, taking the consideration of power consumption not security as a goal. As security plays an important role in the ability to deploy and retrieve trustworthy data from a WSN. This paper introduces all kind of routing protocols with their advantages and disadvantages. We also present a survey of all kind of attacks and secure routing protocols which will help us to know about the present status of security in WSN. We also introduce the concept of multipath routing in WSN to provide the secure and reliable communication. At the end we have proposed the solution regarding security point of view for WSN.***

Keywords: wireless sensor network (WSN), routing protocol, secure routing protocol, multipath routing.

1. INRODUCTION

Wireless sensor network consists of large number of small, low power, low cost sensor nodes with limited memory , computational and communication resources and a base station. These nodes continuously monitor environmental conditions and collect detailed information about the physical environment in which they are installed, and then transmit the collected data to the BS. BS is the gateway from sensor network to the outside world. The BS has a very large storage and large data processing capabilities. It passes the data it receives from sensor node to the server from where end-user can access them. The sensor nodes are generally deployed around the area of base station and forms group as per the need of the Base station [1].

The sensor node is made up of four main parts:

i) A power unit, consisting of a battery and a number of DC/DC converters.
ii) A processing unit which usually consists of a smaller processor and memory.
iii) Physical sensors.
iv) The transceiver circuit, a radio system that should be formed by a transmitter and a receiver.

The processing unit (PU) is responsible for reading out the physical sensor, extracting relevant information from the digitized data and implementing the network protocols. The PU of a wireless sensor node determines both the energy and the computing capabilities of a sensor node. The radio system allows wireless communication between the nodes in the network and the outside world.

Battery is a complex element whose operation depends on many factors including the size of the battery, the electrode material and the rate of diffusion of the active materials in the electrolyte [2]. GPS(global positioning system) is also included in the components of sensor node and ADC(analog to digital converter) is also the part of sensor node. Figure 1. Shows the components of sensor nodes.

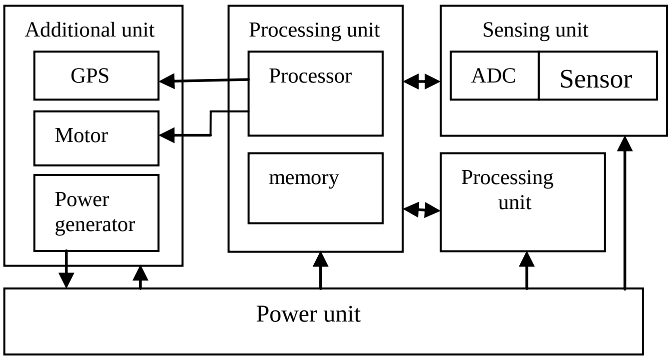


Figure 1: components of sensor node.

Now we can say in simple words that the concept of wireless sensor network is based on a simple equation:
Sensing + CPU + Radio systems = thousands of potential applications.
As soon as people understand the capabilities of wireless sensor network, hundreds of applications spring to mind. There are countless applications in many different fields, including: **Environmental monitoring**, it contains air pollution monitoring, forest fire detection, landslide detection,
Water quality monitoring and natural disaster prevention**. Area monitoring,** in this WSN is deployed over a region where

some phenomenon is to be monitored. A military example is the use of sensors detects enemy intrusion. **Healthcare monitoring**, in this sensor nodes senses body pressure measurement and location of the person, overall monitoring of ill patients in hospital and at homes. **Industrial monitoring**, it contains machine health monitoring, data logging, water/waste water monitoring and structural health monitoring [3].

The main objective of this paper is to focus on the security aspects in WSN. Sensor networks are based on wireless networks so there are easily affected in security point of view as compared to wired network. This paper covered all the types of attacks, secure routing protocol, multipath concept in WSN and the proposed solution which will be beneficial to improve the security of WSN networks.

II. BACKGROUND

First of all we need to know about all the basic security requirements to proceed further and these are as follows:

- ✓ Data confidentiality: data cannot be reaching by outsider.
- ✓ Data authentication: receiver ensures the data received from a trusted source.
- ✓ Data integrity: data is exchanged without malicious alteration.
- ✓ Data freshness: prevent identical copies of the same message to be sent.
- ✓ Non repudiation: this service prevents the sender or receiver from denying the sent or received message.
- ✓ Availability: service has to be always available means this service is used to prevent the loss of access eg. Due to denial of service attacks [4].

There are number of different threat models to sensor networks like **mote-class attackers & laptop-class attackers** and another one is **outside attacks & inside attacks [5]**. In mote-class attacks the attackers has access to few sensor nodes. Whereas the laptop-class attackers are assumed to have much stronger computational capabilities and longer radio range, if they are equipped with hardware powerful enough, the radius of their monitoring area could even cover the entire network. The laptop-class attackers can eavesdrop on all communication in a sensor network. On the other hand outside attackers are the attackers that are external to the network, mote, laptop and inside attackers can be situated in the network in the form of authorized node but actually it will be the malicious node.

There are some network layer attacks in sensor network and these are as follows:

a). Spoofed, altered or replayed routing information:

Definition: attacks against the routing information exchanged between nodes.

Actions: spoofing, altering and replaying routing information.

Results: creating routing loop, attract or repel traffic, extend or shorten sources routes, generate false error message and partitioning the network.

b). Selective forwarding:

Definition: in this kind of attack the malicious nodes try to stop the propagation of certain messages.

There can be the two conditions in this process first one is when adversaries are on the path of flow.

Actions: refuse forwarding certain messages, drop certain messages suppressing or modifying packets from a selected few other good nodes.

The second condition is when the adversaries overhear a flow. In this case the actions can be: jam or cause collision on each forwarded packet.

Results: suppress certain messages.

c). Sinkhole attacks:

Definition: adversaries attract nearly all traffic from a particular area through a malicious node. thereby creating sinkhole with adversary at the centre. After receiving whole network traffic it modifies the secret information.

Actions: tamper with application data along a packet flow path, sending out strong signals with low latencies, laptop-class adversary provide a high quality route to base station by transmitting a high power, creating a wormhole using wormhole attack.

Results: suppressed messages in a certain area.

d). Sybil attacks:

Definition: A single node forges multiple identities.

Actions: having a set of faulty entities [6].

Results: reduces the efficiency of fault- tolerant schemes.

e). Wormhole attacks:

Definition: Adversaries tunnel messages over alternative low latency links and replay them in a different part of the network [7].

Actions: an attacker locates between two nodes and forwards messages between them.

Results: exploits routing race conditions, enable other attacks(eg : create sinkhole) ,convince two distant nodes that they are neighbours, combine with selective forwarding or eavesdropping.

f). HELLO flood attacks:

Definition: An attacker sends or replays routing protocols HELLO packets with more energy.

Actions: in this an adversary which is not a legal node in the network, can flood hello request to any legitimate (genuine) node and break the security of WSN.

Results: the network is at the state of confusion; attract a lot of nodes to use the forged high-quality routes.

g). Acknowledgement spoofing:

Definition: spoof link layer acknowledgement to trick other nodes to believe that a link or node is either dead(actually alive) or alive (actually dead).

Actions: spoof link layer ACK packets of neighbour nodes, selective forwarding by encouraging sender to send via weak links.

Results: convince a sender that a weak link is strong, convince a sender that a dead of disable node is alive, can create a selective forwarding attack.

h). Denial of service attack:

Definition: an event that diminishes or eliminates a network's capacity to perform its expected functions
Action: by the help of attackers they can interfere the sensor network protocols.
Results: they can jam a network on node's performance, can create misunderstanding in between the transmission and can create routing loops [4].

111. RELATED WORK

In WSN routing protocols [8] provide different mechanisms to develop and maintain the routing tables of the nodes of the network and find a path between all nodes of the network. And also find out the best route to a given destination. All of the proposed routing protocols are easily effected by different kind of attacks. There are so many routing protocols which have been already developed such as TinyOS beaconing protocol, Geographical and energy aware routing protocol(GEAR)[9], Greedy perimeter Stateless routing(GPSR),low energy adaptive clustering hierarchy(LEACH)[10], Threshold sensitive energy efficient sensor network(TEEN)[11],Power efficient gathering in sensor information sysyem(PEGASIS)[12] and some energy conserving topology maintenance protocols such as SPAN[13],GAF[14] etc . But these protocols are vulnerable to many types of attacks. Table 1 shows the summary of attacks against proposed sensor network routing protocol.

TABLE 1 . Attack against routing protocols

Protocols	*Attacks*
TinyOS beaconing	HELLO flood, Sybil, wormholes, sinkhole, selective forwarding ,bogus routing information.
Rumor routing	Sybil, sinkhole, wormhole, selective forwarding, bogus routing information.
Energy conserving topology maintenance (SPAN,GAF, CEC,AFECA)	Sybil, bogus routing information, HELLO flood attack.
Clustering based protocols(LEACH,TEEN, PEGASIS)	HELLO flood, selective forwarding.
Minimum cost forwarding.	Selective forwarding, sinkholes, wormholes, HELLO flood, bogus routing information.
Geographic routing(GPSR,GEAR)	Sybil, selective forwarding, bogus routing information.
Direct diffusion and its multipath variant	HELLO attack, bogus routing information, Sybil, wormholes, selective forwarding, sinkholes.

In this section we will pay attention to already proposed security routing protocols with their advantages and disadvantages. Adrain Perrig et. Al [15] proposed SPINS security protocol for security aspects. This consists of two parts: SNEP and uTESLA. SNEP provides data confidentiality, data authentication and data freshness where as utesla provides authentication. For data confidentiality they use symmetric encryption mechanism in which same key called master key is used between sensor node and base station. SNEP uses one time encryption key that produces from the unique master key.
Disadvantages:

- SPINS is based on binary security model means either it provides maximum security or no security.
- In SPINS number of security key is directly proportional to the number of nodes in the network so it has scalability issues.
- It can only work with non-anonymous environment.
- It does not address security in physical layer.
- It does not provide data integrity, availability and non-repudiation security requirements.

Chris Karlof et. Al [16] have proposed TenySec architecture for WSN. It provides the security at link layer so it provides data authentication, data integrity and data confidentiality.
Disadvantages:

- It does not provide protection against physical layer attacks.
- It does not provide access control and non repudiation.
- Like SPINS it also works with non-anonymous environment.
- Its major drawback is that it is tightly coupled with Berkeley TenyOS and cannot be used for general sensor network model[17].

K. Jones et. Al [18] have proposed the solution for providing differential security services for WSN by using parameterized frequency hopping and cryptographic key mechanism..it provides integrity, confidentiality and availability for anonymous nodes.
Disadvantages:

- It does not provide access control and non-repudiation.
- They do not provide direct authentication mechanism.

Taejoon park and Knag G. Shin [19] have proposed light weighted security protocol(LiSP) that gives a trade off between security and energy consumption through efficient re-keying mechanism. LiSP provides authentication, confidentiality, availability, access control and integrity. By using it each node need to save eight keys.
Disadvantage:

- It does not provide non-repudiation.

Sencun Zhu et. Al [20] have proposed localizes encryption and authentication protocol(LEAP).The design of this protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and that a single key mechanism is not suitable for meeting these different security requirements. LEAP supports the establishment of four types of keys for each sensor nodes- an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighbouring nodes and the group key that is shared by all the nodes in the network. It provides data authentication, integrity and confidentiality.
Disadvantages:

- It only works in static environment where the nodes are not mobile.
- It does not provide access control, non-repudiation and availability.

IV. CONCEPT OF MULTIPATH ROUTING PROTOCOL IN WSN

In this section we are going to discuss the concept of multipath routing with its benefits. Nowadays multipath routing [21] approach is widely used in wireless sensor networks to improve network performance through efficient utilization of available network resources. Due to the capacity of multi-hop path and the high dynamics of wireless links, single path routing approach is unable to provide efficient high data rate transmission in WSNs. The multipath routing approach is broadly utilized as one of the possible solutions to cope with these limitations. The reasons behind using these multipath routing protocols are as follows:

a). Reliability and fault tolerance :

The main idea behind using multipath routing approach in WSN is to provide path resilience (against node or link failure) and reliable data transmission. By using this mechanism, as long as an alternative path is available from a target area towards the sink node, data forwarding can be continued without any interruption even in the case of path failure. In the fault tolerance domain, whenever a sensor node cannot forward its data packets towards the sink, it can benefit from the availability of alternative paths to salvage its data packets from node or link failures.

b). Load balancing and bandwidth aggregation:

According to the resource limitations of wireless sensor nodes, intensive traffic loads in high-data rate applications are prone to congestion, which highly influences the network performance. In load balancing method, spreading the traffic along multiple routes can reduce congestion in some links and bottlenecks. In bandwidth aggregation method the effective bandwidth can be aggregated. This method is beneficial when a node has multiple low bandwidth links but it require a bandwidth that is greater than the one which an individual link can provide.

c). QoS improvement:

QoS support in terms of data delivery, end-to-end latency and network throughput ratio is an important objective in designing multipath routing protocols for different types of networks.

After the describing the benefits of multipath routing protocols, we describes elements of multipath routing protocol. There are three main components of multipath routing protocols: path discovery, traffic distribution and path maintenance [22]. The main task of path discovery process is to determine a set of intermediate nods that should be selected to construct several paths from the source nodes toward the sink node. Once a set of paths are selected among the discovered paths, the multipath routing protocol should determine how to distribute network traffic over the selected paths. Based on the primary motivation behind the design of different multipath routing protocols they may utilize various traffic allocation mechanisms. For instance, transmission reliability can be guaranteed by introducing a certain degree of data redundancy in the data delivery process based on the reliability requirement of the underlying application. After that, the source node will utilize several paths to forward generated network traffic towards the sink node. Path maintenance is also the important element of multipath routing protocols .Due to the resource constrains of sensor nodes and high dynamics of low-power wireless links, paths are highly error prone. Therefore, path reconstruction should be provided to reduce performance degradation. This is the main task of the path maintenance phase in multipath routing protocols. Path rediscovery process can be initiated in three different situations: (1) when an active path has failed, (2) when all the active paths have failed or, (3) when a certain number of active paths have failed.

V. PROBLEM STATEMENT

WSNs have many characteristics that make them very vulnerable to malicious attacks. These are:

- A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
- Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
- Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and Performance. However, attackers can break weak security protocols easily.
- A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment.

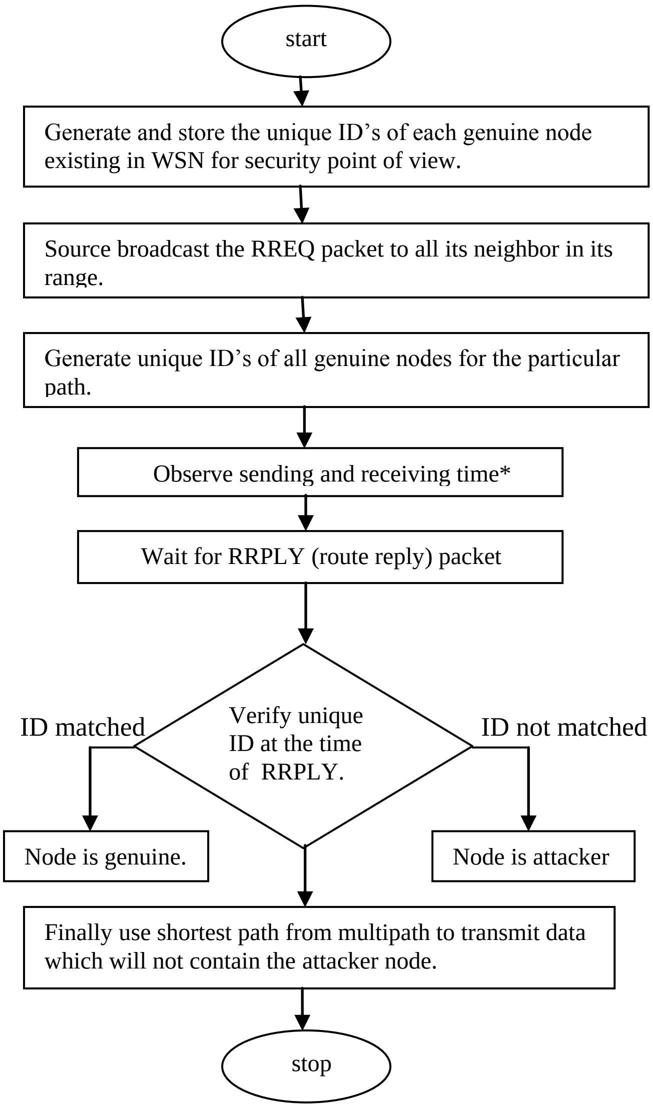
  Therefore, a WSN may face various attacks.

The problem, detection of the malicious nodes, has been addressed separately in different protocols, which are either extensions or based on secure routing protocols. In this work we are going to find out the attacker node from our WSN so that our network could be free from all the attacker nodes.

VI. PROPOSED SOLUTION

In our work we are giving the solution, in which we are not using the key concept like pair key, triple key or anything else because in the management of keys, lots of energy of sensor node is used and then at secure data transfers from source to destination the energy of sensor nodes also used. We want to give the secured routing algorithm which provides secured data transfer as well as find attacked node or exposed node also and also take less energy which is called energy efficient. The main

aim of this work is to send the data from source to destination with full security so that any attacker can not interrupt our data in between the path. Here we are going to remove the wormhole attacker which may be inserted in between our network while processing. In wormhole attack, an attacker node sniffs packets at on in the network, tunnels the packets through a wired or wireless link to another point and in between the transmission node can make any kind of harm to our data or packet. So because of this malicious activity such kind of attacker node takes more time to send the packet from one node to another. This kind of attacker can insert any time in between our network. To find out these kind of attacker node we have proposed this solution. In our work first of all we will generate the unique ID of each and every node for security point of view by using hash algorithm. Then the source will send the route request (RREQ) packet to all its neighbor. We also have the unique ID verification at the end of our proposed solution .At the end we will apply the verification method on the route reply (RRPLY) packet for confirmation of genuine node. Finally we get multipath and we will choose the shortest path for our data transmission from source to destination. We can simplify our work by giving its flow chart:


start
Generate and store the unique ID's of each genuine node existing in WSN for security point of view.
Source broadcast the RREQ packet to all its neighbor in its range.
Generate unique ID's of all genuine nodes for the particular path.
Observe sending and receiving time*
Wait for RRPLY (route reply) packet
Verify unique ID at the time of RRPLY.
ID matched
ID not matched
Node is genuine.
Node is attacker
Finally use shortest path from multipath to transmit data which will not contain the attacker node.
stop

*We will assume the particular time for packet transmission from one node to another. The attacker node will take more time than genuine node because of some malicious activity. Then we can simply say that the node which takes more time in transmission will be the attacker node but it can be possible that because of congestion the genuine node took more time in transmission of packet. So for that confirmation we will apply verification step at RRPLY.

VII. CONCLUSION

In this paper, we have presented the components of sensor node. We discussed different requirements of security with different kinds of attacks in WSN.

Different security protocols have been discussed and we found that none of the solutions provide complete security and most of them are easily effected by different kinds of attacks. We have also included the multipath concept of WSN with its benefits. We have mainly considered the security problem of WSN which is one of the major issues now a day. At the end we have given our proposed new solution to find out the attacker node in between the network. As part of our future work, we intend to do more research on packet lost concept in between the transmission and we will also evaluate our scheme by simulations and test based experiments.

VIII. REFERENCE

[1] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey". Computer Networks, Vol 52, Issue 12,Pp. 2292-2330, August 2008

[2] M. Hempstead, M. J. Lyons, D. Brooks, and G-Y Wei,"Survey of Hardware Systems for Wireless Sensor Networks", Journal of Low Power Electronics, Vol.4,pp.1–10, 2008

[3] D.Puccinelli and M.Haenggi WSN: applications & Challenges of ubiquitous sensing IEEE CAS magazine, sep. 2005

[4] Riaz A . Shaikh, Young Jae Song, Sungyoung Le ,Securing Distributed Wireless sensor Networks: Issues and Guidelines " , Computer Eng . Department, Kyung Hee University, Korea Corresponding Author's.

[5] Chris Karlof, David Wagner, University of California At Berkeley, secure routing in WSN: attacks and countermeasures.

[6] J.R.Douceur, "The Sybil Attack", in 1st International Workshop on Peer-to-Peer Systems(IPTPS'02), March 2002.

[7] Y.C,Hu, A.Perrig, and D.B Johnson, "Wormhole detection in wireless ad-hoc networks", Department of Computer Science , Rice University, Tech. Rep. TR01-384, June 2002.

[8] Sandra Sendra, Jaime Lloret, Miguel García and José F. Toledo." Power saving and energy Optimization techniques for Wireless Sensor Networks " Journal Of Communications, vol. 6, no. 6, September 2011

[9] Y.Yu, D.Estrin, and R.Govindan,"Geographical and Energy-Aware Routing: A Recursive data dissemination Protocol for self-organization of a wireless sensor networks", UCLA Computer science department Technical report, UCLA-CSD TR-01-0023, May 2001

[10] W. Heinzelman, A. Chandrakasan and H. Balakrishnan,"Energy-Efficient Communication Protocol for Wireless Microsensor Networks," 33rd Hawaii International Conference on System Sciences (HICSS '00), 4-7 January,2000, Maui, Hawaii.

[11] A. Manjeshwar and D. P. Agarwal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 23-27 2001, San Francisco,California, USA

[12] S. Lindsey, C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", IEEE Aerospace Conference 2002, Vol. 3, Big Sky, Montana, 16 March 2002. Pp. 1125-1130.

[13] B.Chen, K.Jamieson, H.Balakrishnan, and R.Morris,"SPAN: An energy efficient coordination algorithm for topology maintenance in ad-hoc wireless networks", ACM Wireless Networks Journal, vol. 8, no. 5, September 2002.

[14] Y.Xu, J.Heidemann, and D.Estrin,"Geography-informed energy conservation for ad-hoc routing", in Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001.

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar,"SPINS: Security protocols for sensor networks", proceedings of 7th annual international conference on Mobile computing and networking, Rome, Italy, Aug 2001, pp 188-189.

[16] Chris Karlof, Naveen Sastry, and David Wagner, "TinySec: a link layer security architecture for wireless sensor networks",Proceedings of the 2nd international conference on Embedded networked sensor systems , Baltimore, MD, USA, Nov 2004,pp 162-175

[17] Adrain Perrig, John Stankovic, and David Wagner, "Security in wireless sensor networks", communications of ACM, Vol47(6), Jun 2004, pp. 53-57

[18] K. Jones, A.Wadaa, S. Oladu, L. W|son, and M. Etoweissy,"Towards a new paradigm for securing wireless sensor networks", Proceedings of the 2003 workshop on New security paradigms, Ascona, Switzerland, Aug 2003, pp 115 – 121.

[19] Taejoon Park, and Kang G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks' ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, Aug 2004, Pages 634–660

[20] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient Security Mechansim for Large-Scale Distributed Sensor Networks ", Proceedings of the 10th ACM conference on Computer and communications security, Washington, USA, 2003, pp. 62-72

[21] R. Marjan, D. Behnam, A. B. Kamalrulnizam and M. Lee, "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges", **(2012)**.

[22] Mohammad Masdari and Maryam Tanabi," Multipath Routing Protocol in WSN: A Survey and Analysis", International journal of Future Generation Communication and Networking voi.6 No.6 (2013)