International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 12 (December 2014), PP.36-41

A Survey on Secure Hierarchical LEACH Protocol over Wireless Sensor Network

Hemali M. Bhalodiya[1], Sunera Kargathara[2], Mohit Meghani[3]

Abstract:- Wireless Sensor Network contain number of nodes. Lifetime of Sensor nodes depend on their battery power, which cannot be reenergize. Thus, to save the node energy & lifetime of the Network energy efficient LEACH protocol is introduced. Wireless sensor networks are facing many experiments such as the partial source in processing power, storage and energy. The inadequate energy source is one of the main tasks facing the security in such networks. LEACH doesn't shield the safety harms. So we want to improve security scenario of Secure LEACH protocol. Hierarchical or cluster base routing protocol for WSNs is the most energy-efficient among other routing protocols. This paper shows different security mechanism used in LEACH protocol. This all protocol is based on Hierarchical routing protocol. This paper shows basic scenario of security in LEACH.

Keywords:- Wireless Sensor Network, LEACH, attacks, sensor security, cryptography

I. INTRODUCTION

Like living people, a variety of modern plans and tools depend on the sensory facts from the real world nearby it. These sensory facts approaches is provided by Wireless Sensor Networks (WSN), which contains a number of tiny sensor nodes to display physical or environmental conditions, such as temperature, vibration, pressure, sound or motion, and then jointly send these data to a crucial computing system, called the base station or sink. Wireless sensor networks being a setup less wireless network where nodes are self-determining and self-organizing. The main feature of using wireless sensors is because they have motivating faces such as low-power consumption and low cost. [3]

Many uses of wireless sensor networks are planned to observe a change of environments and gather facts. The data is proposed in altered definitions based on their future use. However, promising data privacy, validity, accessibility, and reliability must be maintained. Security is one of the main interesting facets in wireless networks because it has outcome on the sensors resource due to the very partial resources in the wireless sensors. Due to wireless sensor boundaries it is tough to employ predictable security procedures on wireless sensors networks. In WSN, there are many usages that need a high security level. For example, military and health care submissions. Such submissions need supreme security.

However, a growth in security munches more resources. When more resources are disbursed it can harmfully effect the duration of the network. Wireless sensors should have the supreme security with nominal power consumption to comfort secure wireless communication. In literature survey many protocols are introduced. LEACH (Low Energy Adaptive Clustering Hierarchy) is an energy efficient protocol.

II. LEACH

LEACH is the main network protocol that procedures cluster hierarchy routing mechanism for wireless sensor networks to enlarge the lifecycle of network. All the nodes are in LEACH form themselves as a local cluster. Among all this node one node act as a cluster-head. This all the non-cluster-head nodes transmit their data to cluster-head node then cluster-head node receive data from all non-cluster-head nodes then perform signal processing functions (e.g. Data aggregation) on data and then transmit it on to the remote base station. Hence, actuality a cluster -head node has plentiful energy-intensive than being non-cluster-head nodes. So, accordingly when a cluster-head node expires all the non-cluster nodes that fit to the cluster loss their communication capacity. The procedure of LEACH is separated into two rounds namely set-up phase and steady-state phase. Each round starts with a set -up phase. In which the clusters are prearranged, followed by a steady-state phase where some frames of data are moved from the non-cluster-head nodes to the cluster -head and then cluster-head to the remote base station. Fig. 1 shows a basic architecture of LEACH protocol. [3]

This Fig. shows basic architecture of LEACH. LEACH is mainly depend on three parameters namely Network Life time, System Throughput, Total Energy Consumption etc. Only LEACH does not give any measure security. Only LEACH does not give accurate result also. So we introduced Secure LEACH mechanism in this paper. In this paper, we afford different security methods to LEACH protocol after signifying the source and limitation of nodes. We also introduced different Security Mechanisms also to detect and prevent different attacks in protocol. This is very important in LEACH protocol. [3]

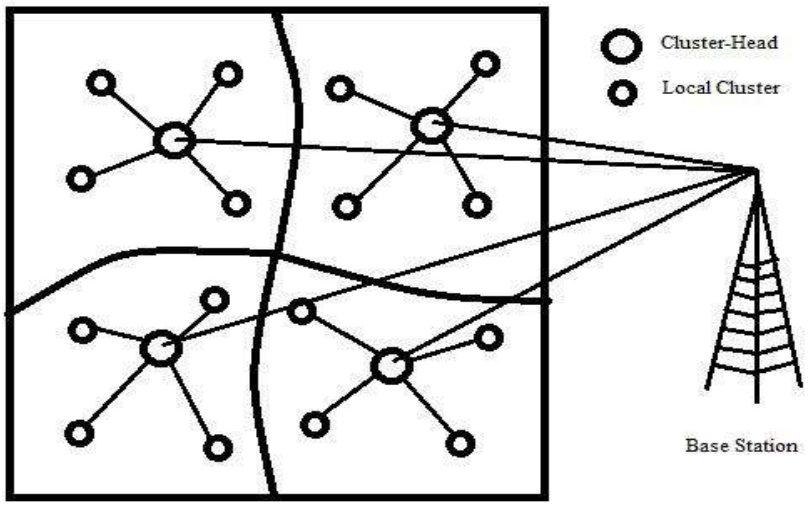

Fig.1 LEACH Clustering Hierarchy

Similarly, we change the security methods to protect wireless sensors and the communications from possible attacks without negotiating the network performance. For example, securing LEACH protocol against denial of service attacks while keeping up its performance. Moreover, the protocol declares that only the authenticated nodes are certified to join and conversed in the network. At the further point, we moderate the overhead cost from the security measures applied to escape negotiating the network performance.

II. SECURITY GOALS IN WSN

In a real world, we guarantee the security aim if every suitable node collects all the messages proposed to it. In the attendance of resourceful adverse, security aims agreement the confidentiality, integrity, authenticity, availability and freshness of data. Mainly, security contracts with providing the following facility in the network:

- **Data Confidentiality:** This things confirms that sensed and transferred data is never exposed to unofficial nodes. Data secrecy can be accomplished in hop by-hop or end to-end basis. While interconnecting the data in the network, no other can understood except proposed recipient. There is a one standard method to keep the delicate data secret is to use the cryptography technique, therefore we can achieve the confidentiality. [4]
- **Data Integrity:** Confirms that the content of a message has not been changed, either intended to harm or by accident, during transmission procedure Data should reach to the proposed receiver without any change in the data. Data depletion or damage can even happen due to the communication environment. Reliability of the data can be preserve by the techniques like message digest and MAC. [4]
- **Authentication:** Permits the receiver to confirm that messages are sent by the usable sensor nodes Authentication is essential for sustaining the network, synchronizing with the sensor node and sending or receiving the information. Authenticity can be sustained by the cryptography mechanism like MAC. [4]
- **Availability:** Availability confirms that the facilities of a network should be presented always even in presence of an inner or exterior attacks such as a denial of service attack (DoS). Different mechanisms have been planned by the researches to accomplish this goal. [4]
- **Freshness:** Freshness implies that receiver receives the latest and new data and confirms that no adversary can rerun the old data. This necessity is specifically important when the WSN nodes use shared keys for message communication, where a probable adversary can introduce a rerun attack using the old key as the new key is being refreshed and broadcasted to all the nodes in the WSN. [4]

III. ATTACKS ON ROUTING LEACH PROTOCOL

Many wireless sensor network routing protocols were very simple and easy and not established as security in mind at that level, so the adversary can present different attacks in the wireless network. Mostly network layer protocol (i.e. LEACH routing protocol) suffers from many different attacks like; spoofing or altering the route information, selective forwarding, sinkhole attack, wormhole attack, Sybil attack, HELLO flood attack etc.

4.1Spoofing, Altering or replaying the route Information:

An opponent can promote or change the routing information corruption by spoofing, moving or replying the routing information. By this an opponent also can invites or redirects the traffic or information, increases the latency, generate different routing loops or generates false message or error etc. [6]

4.2 Selective forwarding attack:

In the selective forwarding attack, malicious node simply refuse to take a new packet and then this node drop it simply. If an opponent node drops the whole received packet, it performs like a black hole attack. An opponent clearly includes on the path of data flow to accomplish selective forwarding. [6]

4.3 Sinkhole and Wormhole attack:

Mostly both sinkhole and wormhole attacks are the same. There is a little bit difference between them. Mostly, in this two attacks; the opponent tries to attract or invite all the traffic from a specific area through a negotiated node. Sinkhole attack mostly performs by making a negotiated node look like an attractive to the neighbor or other nodes to route the data packet and generally it will spoof, modify or drop the packet. So from this way, sinkhole attack provide birth too many attacks like; selective forwarding, tempering the routing information etc.

An opponent promote wormhole attack with two different distant malicious nodes and try to attract or invite the traffic by displaying one hop distance to the sink or base station. From this two attacks, Wormhole attack is very tough to discover because it uses out-of-bound channel to route packets in whole network. [6]

4.4 Sybil attack:

In this Sybil attack, a single node represent or shows a multiple identities to the other different nodes in the network. This node tries to mislead the node in neighbor recognition, route information and topology maintenance. This Sybil attack is generally a significant risk to many geographic and multipath routing protocols in wireless sensor network. [6]

4.5 HELLO flood attack:

In this HELLO flood attack, an opponent retransfer overhead packet with sufficient power to be received by each node in the wireless sensor network. The other protocols which generally use the local topology or method like neighbor information for route formation and topology maintenance get affected by this HELLO flood attack.

This all type of attacks are generally introduce in wireless sensor network. We have to solve this problem by using security mechanism in a network. [6]

IV. RELATED WORK

Now a day, Security problems in WSNs are facing many challenging particularly the matter of network availability in wireless field. Securing wireless sensor networks has been very active research in today's era. It became more necessary to provide solution for outsider attacks which are related to Data Confidentiality, Data Integrity, Authenticity, Availability, and Freshness.

In [1] this paper, Alshowkan, Elleithy, Al Hassan, proposed new Secure LEACH protocol named as LS-LEACH. In this paper they provide security measures to LEACH protocol after including the source and limitation of nodes. They provide two encryption key for security. They include Group Key between Cluster Head and Local Cluster nodes and Private Key between Cluster Head and Base Station. They also provide securing

LEACH protocol against denial of services while maintaining its high performance. They also include that only the authenticated nodes are allowed to join and communicated in the network. At last they concluded that LS-LEACH protocol is better than other protocol in terms of system throughput, network life time and the total energy consumption. This LS-LEACH protocol provided a secure authentication protocol for the network.

This paper [2] provides description of LEACH and how LEACH can be compromised by Black hole and Gray Hole attacker. In Black Hole attack the attacker node tries to collect most of the data of the network then drops it. In this Black Hole attack attacker is having higher initial energy so it will become CH in the first round and even in later rounds, so it becomes CH in all the rounds. Then, these attackers do not forward this information to the base station. In Gray Hole attack, attacker simply drops packets coming from local cluster nodes in the wireless network while forwarding all the packets for different nodes. Sometimes node may be look like a malicious node then it became normal node again. This paper concluded that both the attack results in major packet drop. These papers also include that effect of this type of attack increases with increases in network size. The malicious node can affect the information of more nodes. This paper also included that the effect of Gray Hole attacker is less compared to Black Hole attacker. These papers just give a comparison of Gray Hole attack and Black Hole attack.

This is the modified version of SLEACH. This paper [5] proposes MS-LEACH to improve the security of SLEACH by providing data confidentiality and node to CH authentication using Pairwise keys shared between CHs and their cluster members of that group. MS-LEACH offers Pairwise key with no communication overhead in accumulation to the two Symmetric keys used in S-LEACH. A Pairwise key is used for communication between node and CH. In this counter value is added in every round for data encryption. This protocol deals with the orphan node. This is the only limitation of this protocol.

Di Wu, Gang Hu, Gang Ni [8] presented a new secure hierarchical protocol called SS-LEACH, which is the new secure version of LEACH. SS-LEACH is basically depends on Cluster-Head. SS-LEACH develops the method of selecting cluster heads and forms dynamic stochastic multi-paths cluster heads chains to communicate to the remote base station. In this way SS-LEACH improves the energy-efficiency and therefore it can prolong the lifetime of the network. It used the key pre-distribution mechanism and self-localization technique to secure data in the basic LEACH protocol. It also help to stop compromised node to take part in the network and preserve the privacy of the packet. It also avoids several attacks like selective forwarding, HELLO flood attack and Sybil attack.

In this paper, they introduced new secure protocol named as RLEACH [9] which is secure version of LEACH. In RLEACH, Cluster-Head are formed dynamically and periodically. In RLEACH the orphan node problem is increased which is one type of attacker. Due to this random pair-wise key scheme so they have introduced improved random pair-wise key scheme to overcome this problem. RLEACH has been used the one way hash chain. RLEACH also used symmetric and asymmetric cryptography technique to provide security in the LEACH Hierarchical routing protocol. RLEACH fights too many attacks like spoofing, altering and replaying information, sinkhole, wormhole, selective forwarding, HELLO flood attack and Sybil attack.

L. B. Oliveria [11] proposed SecLEACH, a protocol which is used for securing node to node communication in LEACH based network. It used random key pre-distribution mechanism with symmetric key cryptography to develop security in LEACH protocol. This SecLEACH provides Data integrity, Data Authentication, Confidentiality and Freshness to node to node communication. This SecLEACH is vulnerable to node capturing attack. This paper concludes that SecLEACH bootstraps its security from random key predistribution mechanism and it gives performance analysis and gives security scenario. This SecLEACH also shows that the overhead incurred by SecLEACH is manageable.

This protocol is the first modified secure version of LEACH protocol called SLEACH [12], which is used for examine the problem of adding new security parameter to cluster-based communication LEACH protocol for wireless sensor networks which is consisting of sensor nodes with severely limited resources. SLEACH used three method for security in LEACH. So it provides security in LEACH by using the building block of SPINS (Security Protocol for Sensor Network), symmetric-key methods

and MAC (Message Authentication Code). SLEACH protects against many attack like selective forwarding, sinkhole and HELLO flood attacks. It also stops attacker to send fake sensor data to the CH and then CH to forward that fake message to Base Station. But there is one limitation of SLEACH that it cannot stop to crowd the time slot schedule of a cluster. So SLEACH is causing DoS attack or simply dropping the throughput of the CH and SLEACH does not sure about data confidentiality. The solution for this is meant to protect only outsider attack. This is the first mechanism for securing data in LEACH protocol.

V. CONCLUSION

Routing protocol affects the performance of the network in the terms of energy efficiency, security, resiliency and lifetime. So that secure, robust and efficient routing protocol is the basic requirement of this LEACH protocol. In this paper, we have studied and analyzed a number of secure and energy efficient hierarchical routing protocol used in WSNs. In this all protocol, LS-LEACH is higher secure rather than other secure protocol. It is also energy efficient than other protocols. But there is one limitation of this protocol. It use Symmetric key and Asymmetric key both for data encryption. So key management issues are there. So that energy consumption is more compare to use only symmetric key.

ACKNOWLEDGEMENT

I would like to extend my sincere thanks to supervisor **Asst. Prof. Sunera Kargathara**, Department of Electronics and Communication Engineering for her constant support and guidance throughout the research work. As my supervisor she has constantly encouraged me to keep focused on achieving my goal. I am thankful to her to give me her valuable time and sharing her idea and thought about this research area. I also give thanks to co-guide **Asst. Prof. Mohit Meghani** to give me his constant valuable time.

REFERENCES

[1]. Muneer Alshowkan, Khaled Elleithy, Hussain AlHassan, "LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks", in Distributed Simulation and Real Time Application, pages 215-220, IEEE International Symposium, 2013.

[2]. Meenakshi Tripathi, M.S.Gaur, V.Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", in 8th International Symposium on Intelligent System Techniques for Ad Hoc and WSN, pages 1101-1107, 2013.

[3]. Meena Malik, Dr. Yudhvir Singh, Anshu Arora, "Analysis of LEACH protocol in Wireless Sensor Networks", in international journal of Advanced Research in computer science and Software Engineering, Volume 3, Issue 2, pages 178-183, 2013.

[4]. Mohammad Masdari, Sadegh Mohammadzadeh Bazarchi, Moazam Bidaki, "Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks", in journal of network and computer application, Elsevier, pages 1243-1260, 2013.

[5]. Mona El_Saadawy, Eman Shaaban, "Enhancing S-LEACH Security for Wireless Sensor Networks", in Electro/Information Technology (EIT), IEEE conference, pages 1-6, 2012.

[6]. Suraj Sharma, Sanjay Kumar Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks", in International Conference on Computer and Computational Sciences, pages 146-151, 2011.

[7]. J. J. Lotf, M. Hosseinzadeh, and R. M. Albuliev, "Hierarchical routing in wireless sensor networks: a survey", In 2nd International Conference on Computer Engineering and Technology, pages 650–654, April 2010.

[8]. Di Wu, Gang Hu, Gang Ni, "Research and Improve on Secure Routing protocols in Wireless Sensor Networks", in 4th IEEE International Conference on circuits and systems for communications, pages 853-856, 2008.

[9]. Kun Zhang, Cong Wang, Cuirong Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management", in 4th IEEE international conference on Wireless Communications, pages 1-5, 2008.

[10]. R. Srinath, A. V. Reddy, and R. Srinivasan, "Ac: Cluster based secure routing protocol for wsn", In Proc. of the Third International Conference on Networking and Services, page 45, 2007. IEEE Computer Society.

[11]. L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "SecLEACH - A random key distribution solution for securing clustered sensor networks", In 5th IEEE International Symposium on

Network Computing and Applications, pages 145–154, 2006.

[12]. A.C. Ferreira, M. A. Vilaça, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, "On the security of cluster-based communication protocols for wireless sensor networks", In 4th IEEE International Conference on Networking, pages 449– 458, 2005.

[13]. J. N. Al-karaki, A. E. Kamal, "Routing techniques in wireless sensor networks: A survey", IEEE Wireless Communications, 2004.

[14]. Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad-hoc networks, Elsevier, 2003.

[15]. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks" In *Proc.* Of the 33rd Hawaii International Conference on System Sciences (HICSS '00), page 8020, 2000.