Volume 8, No. 4, May 2017 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Protecting Cluster Head from Sybil Attack in Wireless Sensor Networks

Harmeet Singh, Rupinder Singh† and Dr. Jatinder Singh‡

‡SBBS University, Jalandhar. E-Mail: bal_jatinder@rediffmail.com

†Khalsa College, Amritsar. E-mail: rupi_singh76@yahoo.com

‡SBBS University, Jalandhar. E-Mail: bal_jatinder@rediffmail.com

Abstract **- Wireless sensor network routing protocols are basically used to provide the function of data routing towards the sink and are vulnerable to various attacks. LEACH is a one of the routing protocol used for clustered implementation of wireless sensor network with Received Signal Strength based dynamic selection of Cluster Heads. But, as with other routing protocols, the LEACH is also exposed to attacks when the malicious sensor node becomes the Cluster Head by launching Sybil attack. Cluster heads are vulnerable to various malicious attacks and this greatly affects the performance of the wireless sensor network. Cryptographic and non-cryptographic approaches to detect the presence of attack also exist but they lack efficiency in some way. Cryptographic approaches to prevent this attack are not so helpful though some non-cryptographic methods to detect the attack also exist but they are not too efficient as they result in large test packet overhead. In this paper, we propose SRSRP (Sybil Resistant Secure Routing Protocol) extension to LEACH protocol so as to protect the cluster head against Sybil attack. SRSRP is base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of cluster head. The proposed technique is implemented in NS2, the experimental results clearly indicate the proposed technique has significant capability for the detection of Sybil attack launched for making the malicious node as the cluster head.**

Keywords: Wireless sensor networks, LEACH, Sybil attack, Armstrong number, AES, Encryption, Decryption, Cluster head.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are self-configured and infrastructure-less wireless networks to monitor environment or physical conditions, such as temperature, sound, humidity and so on. WSNs cooperatively pass their data gathered through the network to a centre location called base station so that the data can be analyzed for further processing. WSN are deployed in the environments that are usually unfriendly and unsafe. WSNs have a large number of constraints from which results in new challenges. The sensor nodes have unreliable communication medium and extreme resource limitations which make it very difficult to deploy security mechanism. Figure 1 shows the structure of a typical WSN. Most of the protocols for WSNs in the past assumed that all nodes are trustworthy and cooperative. But this is not the case for many sensor network applications today and a variety of attacks are possible in WSN including Hello flood, Wormhole, Sybil, etc.

Sybil attack in WSNs is one of the main attacks in which malicious node intentionally and illegally presents many forge or false identities to other sensor nodes. This is done

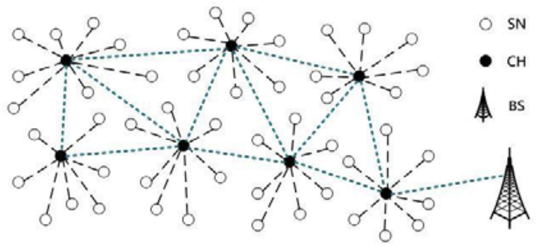

Figure 1: A typical WSN

by either creating new (fake) identities or by stealing legal identities from others sensor nodes. A variety of countermeasures against Sybil attack are proposed in the literature that we discussed in our previous work [1]. Each of the countermeasures has its own limitation and need improvement for producing more efficient one.

Heinzelman et al. [2] introduced a dynamic hierarchical clustering protocol called LEACH (Low Energy Adaptive Clustering Hierarchy) protocol for sensor networks. LEACH divides the WSN into small clusters of which one is the Cluster Head (CH) and others sensor nodes are the cluster members. The cluster sensor node members send their gathered data to the CH, which in turn send it to the Base Station (BS) by aggregating all the received data from its cluster members so as to reduce the redundancy. In LEACH the CH sensor nodes are periodically re-elected so that the same sensor node is not repeatedly used for the high energy job of the CH. LEACH operations are divided into two phases of Setup phase and Steady phase. In the setup phase, the formation of clusters with CH and cluster members is done for the WSN while in the steady phase; data are sensed and sent to the BS. The steady phase is longer than the setup phase and is done in order to minimize the overhead cost.

LEACH protocol is a more secure protocol as compared to the conventional multi-hop protocols as in conventional multi-hop

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

protocols, the sensor nodes around the BS are more attractive to compromise as they are the major points of aggregation and forwarders of all packets to the BS. While in LEACH protocol, the CH are the only node that directly communicate with the BS and the location of these CH can be anywhere in the WSN irrespective of the BS. More over these CHs are regularly randomly changed. Therefore, spotting these CHs is very hard for the adversary in WSN. However, as LEACH is a cluster-based protocol, depending exclusively on the CHs for aggregation of data and its routing, attacks on the CH are the most harmful. If any adversary node becomes a CH, then it can make possible attacks like Sybil, Sybil attack, selective forwarding etc.

Hello packets in WSN are used for neighbour discovery but they can be used by a malicious node with high transmission power to launch Sybil attack on CHs in WSN. A Sybil node is created by creating duplicate ID of CH. A number of countermeasures against Sybil attack in WSN have been proposed in the literature that we discussed in our previous work [1]. Most of the proposed countermeasures have limitation and need improvement for producing more efficient one. In this paper, we propose a SRSRP (Sybil Resistant Secure Routing Protocol), an extension to LEACH protocol and is base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of the CH so as to prevent the WSN from Sybil attack. The remaining paper is organised as follows: In section II, we discuss related works; the section III describes the working of SRSRP. In section IV, we provide the simulation of proposed protocol in NS2 while we end with the conclusion in section V.

II. RELATED WORKS

In this section of the paper, we discuss the work proposed in the past for providing secure formation of clusters by LEACH protocol in WSN, and the proposed work for selecting CHs in a secure way.

Heinzelman et al. [2] proposed LEACH in which every sensor has a probability of becoming a CH without message exchange. This technique attempted to extend the network life time by making all sensor nodes play a role of CH. In LEACH, some sensor nodes with a high chance declare themselves as CHs and other sensor nodes join in one of them. Since, this method assumes no compromised sensor nodes in the WSN; it has no method to protect the cluster formation from the malicious sensor nodes. F-LEACH [3] was proposed in order to defend the cluster formation in LEACH protocol. In this proposal, when a sensor node declares itself as a CH, it employs the use of common keys shared with the BS so as to check the authentication of the CH declaration to the BS. Then, the sink securely broadcasts the authenticated CHs using μTESLA [4]. Normal sensor nodes in WSN join in only one legitimate CH. However, this method has no means to validate the normal sensor nodes which join in any cluster. To resolve this problem, Oliveira et al. [5] proposed SecLEACH in which the BS authenticates the CH nodes and further the CHs authenticate the joining sensor nodes. In both F-LEACH and SecLEACH, sensors nodes are pre-assigned some keys for verification before their deployment. However, both F-LEACH and SecLEACH can help in preventing only external attackers from joining of the process of cluster formation i.e. they cannot avoid internal attacks from capturing CHs.

Many extensions to LEACH [7-11] have been proposed in the past but, most of them focus on balancing the consumption of energy over all sensor nodes and extending the lifetime of the network. A few of them [8] deals with electing a CH securely. However, this technique cannot prevent a malicious node from declaring itself as a CH as it can defraud other nodes that it has a short distance to the BS along with a large amount of residual energy. Liu proposed a cluster formation method in which only pre-determined nodes can declare themselves as CHs while other nodes can join any cluster either directly or via a relay node [13]. As any CH declaration or cluster join is authenticated by some pre-assigned polynomial share, the method avoids any external attacker from participating in the process of cluster formation. In this method, a compromised relay node can invoke a Denial of Service (DoS) attack by removing the connection between CH and its serving nodes. Pre-determined CHs become the targets of attackers because their roles are fixed. Sun et al. [14] proposed a protected scheme for cluster formation which checks the protocol conformity of nodes in order to discriminate mean nodes from usual nodes. In this method, physical network is transformed into cliques and members are openly connected to each other in a clique. After the formation of clique, each node checks that all members have the similar view of the clique membership. Even though the method of [19] has enhanced the safety of [14], it supposed that no collisions are possible during the cluster formation. This assumption is difficult to satisfy without the use of any special measure such as TDMA schedule assignment and code separation. Nishimura et al. [21] proposed a method where all nodes allocate a trust value to each candidate of CH and the most trusted nodes are allowed to become CH. Otherwise, the nodes join a close cluster to form clusters in the network. The drawback of this scheme is that it produces a lot of communication overhead for the building of trust evaluation system. So, this method is not appropriate for resource-constrained WSNs.

Rifà-Pous et al. [20] proposed a protected cluster formation method that is based on public key cryptography. The scheme is composed of three phases; cluster discovery phase, CH designation phase, and cluster maintenance phase. In the phase of cluster discovery, all nodes in a cluster have the same view on the membership of cluster with each other. In the phase of cluster designation, a CH is elected considering the number times it performed the CH and number of its neighbours. In the phase of cluster maintenance, the elected CHs provide an authorization certificate to every member in the cluster. But, this method assumes that no nodes depart from the cluster discovery protocol. For example, if a malicious node transmits its message to part nodes in the phase of cluster discovery, the sufferers have a dissimilar view on the membership of cluster. Consequently, it divides a cluster into multiple clusters, and the divided clusters elect their CH respectively in the phase of CH designation. That is to say, this method can produce a lot of clusters under the selective transmission attack. Crosby et al. [21] proposed a trust based CH election design where every node provides a trust value to other nodes according to their behaviour and extremely trustworthy nodes become CHs. Every node's behaviour is calculated by counting the occurrence of successful node transmissions and the occurrence of unsuccessful node transmissions. That is, the more a node succeeds in its transmission, the superior reputation value the node has. During the election of new CH, nodes with a more reputation value are suggested for the role of CH by cluster members and one of these is selected as a new CH. A malicious CH can put in a not guilty victim into a blacklist to take away its candidacy for CH in the cluster that is, with the number of blameless victims rises up, a malicious node can enlarge its winning chance.

Buttyan et al. [22] also proposed a CH selection method which conceals the process of election from outside nodes using cryptographic techniques. However, the concealment works only for external attackers as a compromised node can with no trouble expose the selection result. Moreover, the malicious node can announce itself as a CH even though it is not eligible. Sirivianos et al. [24] proposed the Secure Aggregator Node Election (SANE) protocol in which all eligible CH members in a cluster contribute to the production of a random value and a CH is elected randomly using this random value. SANE is classified into further three sub-schemes according to generating and distributing the random value. They are based on Merkle's puzzle scheme, commitment based scheme, and seed based scheme. Dong et al. [25] proposed a method that prevents outside attackers from taking part in a CH election process through its ID assignment scheme, which firmly binds a node's ID, its commitments, and its polynomial shares. In this scheme, the nodes that do not broadcast participation message for CH election or explicitly transmit a non-participation message are excluded from the CH candidates. The final CH is selected by arbitrarily selecting one node amongst the rest of the candidates. However, an inside attacker can change CH election result by avoiding the distribution of its participation message; it can also generate numerous CH election results by the process of distributing its contribution message only to a subset of CH candidates. Even though this method has a recovery system to combine numerous election results into one result, it requires the voluntary co-operation of the CH candidates.

III. Working of SRSRP

In this section of the paper, we describe our proposed SRSRP for the detection and isolation of Sybil attack in WSN. We first discuss the WSN model and assumption and then we describe the working of proposed protocol.

A. Network Model

The clustered sensor network selected in the paper consists of N static sensor nodes, including CH, member nodes, and BS. CHs are responsible for collecting the information within their clusters and passing it to the BS so as to make decisions and judgments. The formation of clusters is based on LEACH protocol. Every sensor node has a unique identity (ID). Following assumptions of the WSN are used in the proposed protocol SRSRP.

1) Sybil attack node, formed by the compromise of CH.
2) The compromised node has a high transmission power.
3) Except the malicious sensor node, all the nodes in wireless sensor network are isomorphic with the same initial energy, transmission power, computing power and internal storage structure.
4) Once each node's ID is allocated, it cannot be changed.
5) Each sensor node is allocated unique Armstrong number.
6) The sensor nodes of the network consume the same energy in the same stage of the work, e.g. the transmission and reception of data packets in the process of detection.

B. Implementation of SRSRP

The SRSRP is an improved secure extension to the LEACH protocol, so the implementation of the proposed protocol has to take advantage of the characteristic of LEACH clustering. LEACH protocol is mainly divided into two phases of set-up phase and stable phase. In the set-up phase, all the sensor nodes have to follow the two guidelines of fairness criterion and randomness criterion. In fairness criteria all sensor nodes in the network have same probability to become a CH. While in randomness criterion, the election of the CH is done in a random way. The chance for a sensor node to become a CH in the round entirely depends on whether the sensor node has ever been elected as CH in the recent rounds and the percentage of the CH sensor in the WSN. When the election of the CH is over, every member node chooses the cluster to join on the basis of the maximum received signal strength until all the clusters are completed. In general, the implementation of LEACH has a longer stabilization phase.

Each member sensor node is responsible for sensing the surrounding environment and forwarding the data to their respective CHs. After collecting information from cluster member nodes, each CH forwards it to the BS. It is vulnerable for LEACH against Sybil due to these characteristics of clustering. Sybil is a common routing attack in the network in which fake or duplicate IDis created and it broadcasts a large number of hello message with higher transmission power to nodes in the network. Any sensor node that receives the hello message with high signal will consider the malicious node as CH. This malicious node may damage the network by selectively modifying, discarding information received from its neighbours.

C. Determination of malicious CH

The BS maintains record of CHs, cluster members, malicious nodes in the registration table as different sets. The values are updated as per the changes in the clusters and CHs. The initial values of these sets are

Set CH_{node} = {null}, the CHs in the network.
Set CH_{member} = {null}, the members of each cluster in the network.
Set $CH_{malicious}$ = {null}, which means the malicious nodes in the network.

Each sensor node with a certain probability (p) try for becoming CH based on the criterion of randomness and fairness. The sensor node that becomes a CH broadcasts the message of self-clustering in order to attract neighbouring sensor nodes so as to join it. The cluster head CH(i) is selected according to the level of the Received Signal Strength (RSS) to join in a certain range of area. The members of the cluster as calculated by each CH are added to the set CH_{member}.

a) Allocation of unique ID

The BS allocates a unique ID to each sensor in the network. Whenever any sensor node request for becoming CH, it has to send this ID to the BS so that the node identification can be validated.

b) Allocation of unique Armstrong number

The BS also allocates a unique Armstrong number against each ID for each of the sensor node in the network. An Armstrong number is an m-digit base n number such that the sum of its (base n) digits raised to the power m is the number itself. For example number 371 is an Armstrong number as $3^3+7^3+1^3 = 27 + 343 + 1 = 371$ which is equals to number itself. Whenever any sensor node request for becoming CH, it has to send encrypted hello message with this Armstrong number. Table 1 shows example registration table maintained at BS.

Table 1: Registration table at BS

Sensor number	Allocated unique ID	Allocated Random Armstrong Number
001	S01	407
002	S02	153
.	.	.
.	.	.
N		54748

The flowchart in figure 2 describes the working of SRSRP for authentication of CH by the BS.

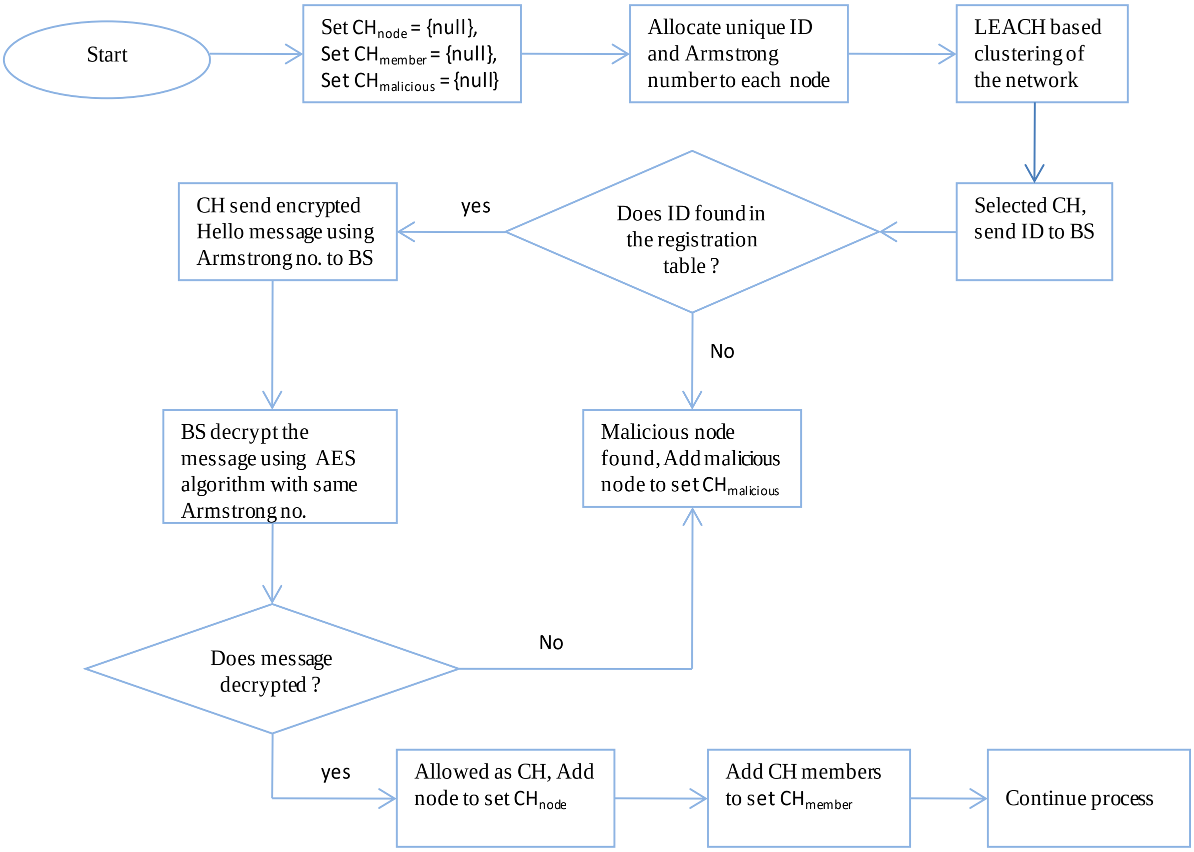

Figure 2: Flow chart of proposed SRSRP

As LEACH is fragile to Sybil attacks because of its characteristics and nature. The compromised non–cluster head sensor nodes have less effect on the performance of network with limit range. But, once it becomes a CH with higher transmission power, a large number of sensor nodes will be appealed for becoming one of its members in a cluster. If the malicious node discards or alters the packets, the circumstances would seriously smash the honesty and precision of the information in the network. The SRSRP can detect the presence of malicious node with fewer energy and small error rate, which can efficiently get better the network performance.

IV. SIMULATION RESULTS

In this section of the paper, we present the results of the simulation to show the effectiveness of SRSRP. The simulation is carried out in ns2.35 with the parameters shown in table 2.

Table 2: Simulation parameters

Parameter	Value
Simulator used	NS 2.35
Area (meter)	800X800
No. of nodes	60
Routing protocol	LEACH
Channel type	Wireless

Packet size	512 byte
Mobility model	Two ray ground propagation model

A. *Throughput*

In the first experiment, we measure the sensor network throughput as this is one of the crucial network parameters. Network throughput refers to the average rate of successfully delivered packets. Throughput is

calculated depending on a total number of packets received at the destination in sensor network per unit of time. Throughput is calculated as

Throughput = (Total number of packets received at the destination) / (simulation time)

Figure 3 shows the throughput analysis in the case of the sensor network without Sybil, under Sybil, and after implementation of proposed SRSRP. The figure clearly shows that the proposed protocol after the isolation of the Sybil results in the increase of throughput.

B. *Packet delivery ratio*

Packet delivery ratio (PDR) of a network is defined as the ratio of the total received packets at the destination to total packets generated by the source node. PDR is calculated as

PDR = (Packets received/packets generated) * 100

Figure 4 shows the PDR analysis in the case of the sensor network without Sybil, under Sybil, and after implementation of SRSRP. The figure clearly shows that the proposed protocol after the isolation of the Sybil results in the increase of PDR. A high value of PDR is an indication that there is less packet loss in the sensor network.

C. *Delay*

The delay is defined as the average time taken by a packet (data) to arrive at the destination. The delay also includes any delay that is caused by the process of route discovery along with queue in data packet transmission. The data packets successfully delivered to the destinations are only counted. It is calculated as:

Delay = ∑ (arrive time – send time) / ∑ Number of connections

The lesser value of delay is an indicator of the better performance of the protocol. Figure 5 shows the end to end delay in the case of sensor network without Sybil, under Sybil, and after implementation of SRSRP. The figure shows that the proposed protocol results in the decrease in end-to-end delay.

D. *Overhead*

Overhead is the excess time taken by the protocol to deliver the packets to the destination. Sybil increases the overhead in the sensor network. The routing overhead is defined as the count of packets used for routing in the sensor network. Figure 6 shows overhead in the case of sensor network without Sybil, under Sybil, and after implementation of SRSRP. The proposed protocol results in decreasing the overhead of the network as shown in figure 6.

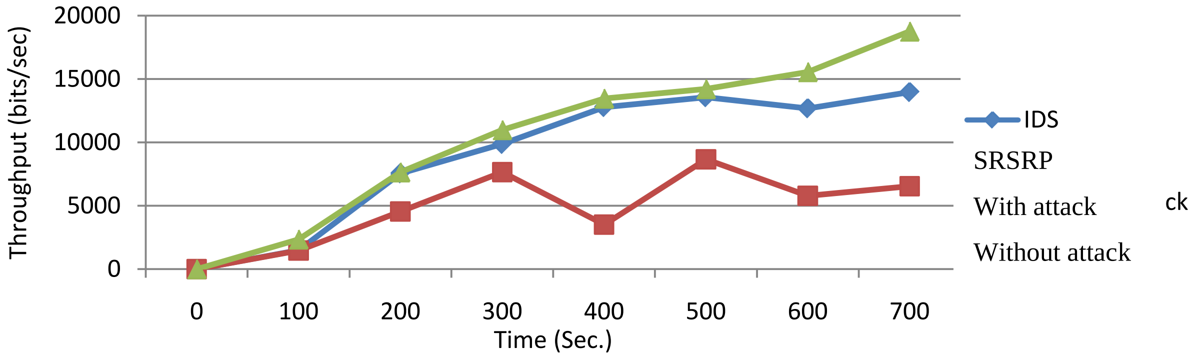

Figure 3: Throughput

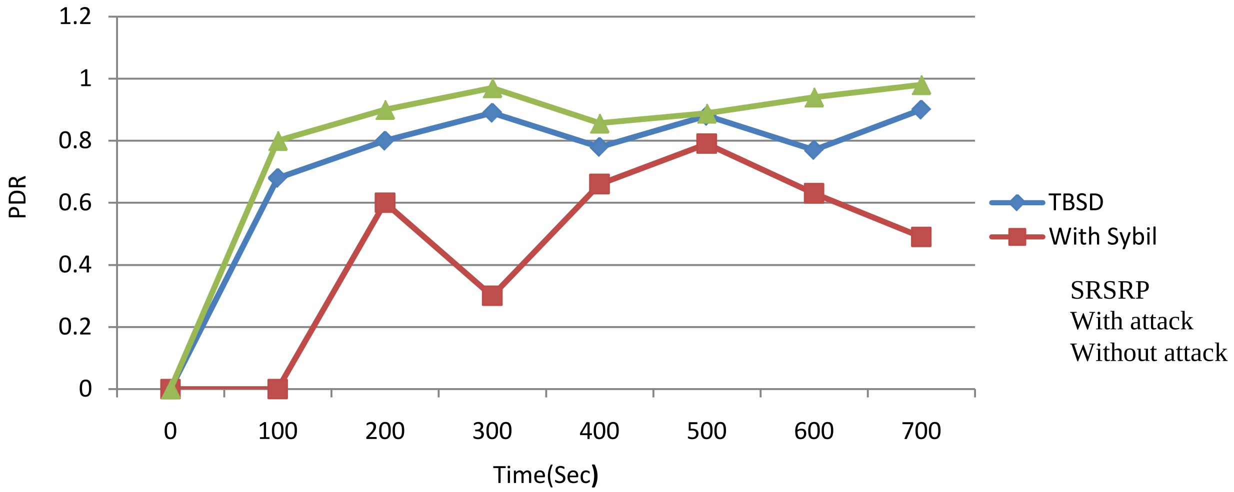

Figure 4: PDR

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

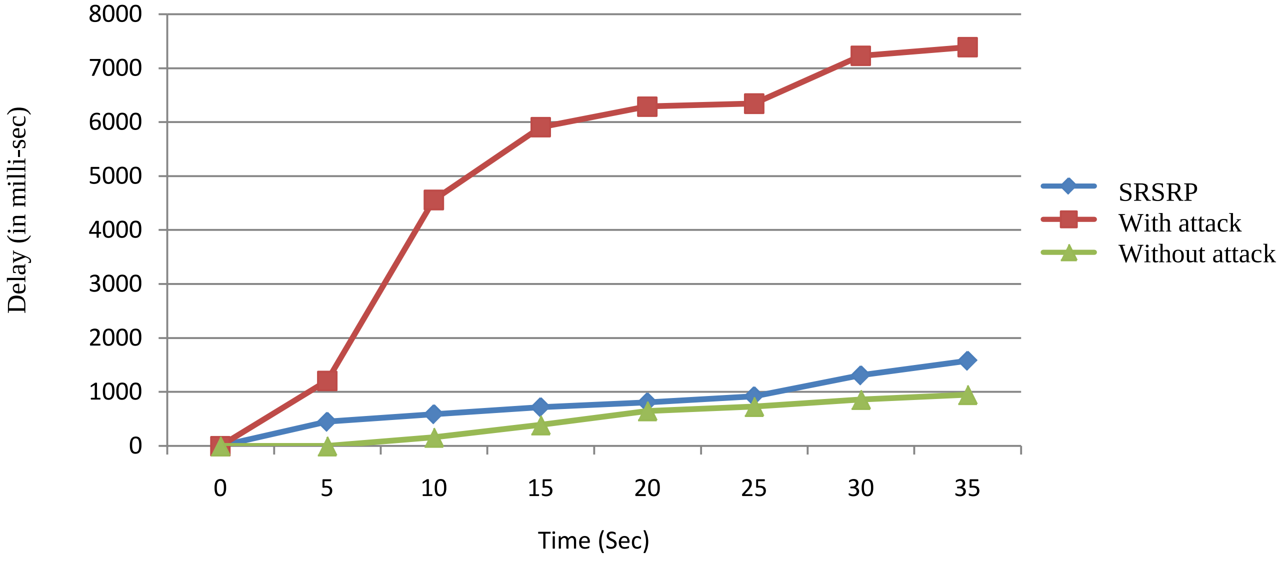

Figure 5: Delay

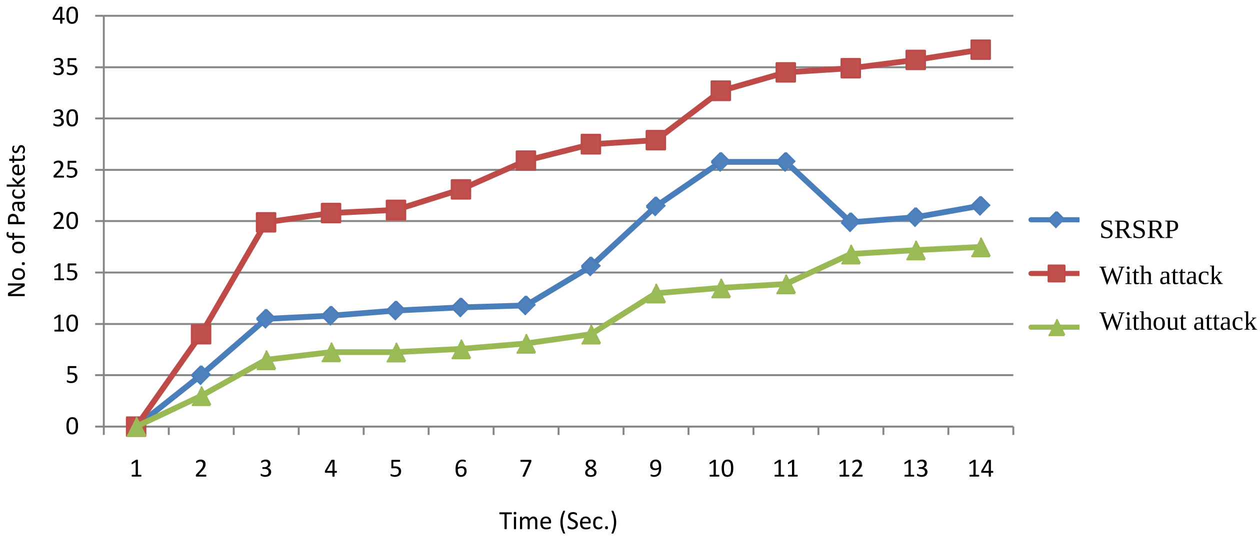

Figure 6: Overhead

V. CONCLUSION

Cluster head selection in a secure way in clustered implementation of wireless sensor network is vital as all the cluster sensor members data to the base station is communicated through cluster head. Sybil in wireless sensor network can be used for making a cluster head compromised by making use of fake or duplicate ID and replaying hello packets which are used for neighbour discovery. LEACH protocol is hard to attack by adversary excluding the case when it can become cluster head. In this paper, a new approach to detect and prevent Sybil in LEACH protocol in wireless sensor networks is proposed. We propose a SRSRP (Sybil Resistant Secure Routing Protocol) extension to LEACH protocol base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of cluster head. SRSRP improves the network performance by early discovery of adversary and preventing the sensor nodes from associating with such a malicious cluster head. The implementation of the proposed technique in NS2 shows its efficiency for the factors of throughput, packet delivery ratio, delay, overhead. The simulation results prove that SRSRP expels more compromised nodes from clusters and suppresses the separation of clusters. Other simulation results also represent that SRSRP raises the quality of clusters and more energy efficient than an opponent scheme. Additional simulation will be done in the future by increasing the number of sensor nodes.

REFERENCES

[1] Rupinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh, “Sybil Attack Countermeasures in Wireless Sensor Networks,” International Journal of Computer Networks and Wireless Communications, Vol. 6, No. 3, May 2016.
[2] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, “Energy-efficient communication protocol for wireless

microsensor networks," In the proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Vol. 2, Jan. 2000.

[3] A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H.C. Wong, and A. A. Loureiro, "On the security of cluster-based communication protocols for wireless sensor networks," Proc. of 4th IEEE Int'l Conf. on Networking, Reunion Island, France, Apr. 17-21, 2005.

[4] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, Vol. 8, No. 5, pp. 521-534, Sep. 2002.

[5] L. B. Oliveira, H.C. Wong, M. W. Bern, R. Dahab, and A. A. Loureiro, "SecLEACH-a random key distribution solution for securing clustered sensor networks," Proc. of 5th IEEE Int'l Symp. on Network Computing and Applications, Cambridge, Massachusetts, USA, Jul. 24-26, 2006

[6] Yaya Shen, Sanyang Liu, Zhaohui Zhang, "Detection of Hello flood attack Caused by Malicious Cluster Heads on LEACH Protocol," International Journal of Advancements in Computing Technology (IJACT), Volume 7, Number 2, March 2015.

[7] S. Kang and T. Nguyen, "Distance Based Thresholds for Cluster Head Selection in Wireless Sensor Networks," IEEE Communications Letters, vol. 16, no. 9, pp. 1396-1399, Sep. 2012.

[8] Y. Han, M. Park, and T. Chung, "SecDEACH: Secure and Resilient Dynamic Clustering Protocol Preserving Data Privacy in WSNs," Proc. of the 2010 Int'l Conf. On Computational Science and Its Applications, LectureNotes in Computer Science, vol. 6018, pp. 142-157, 2010.

[9] V. Katiyar, N. Cand, G. C. Gautam, and A. Kumar, "Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks," Proc. of Int'l Conf. On Emerging Trends in Electrical and Computer Technology, pp. 1070-1075, Mar. 2011.

[10] M. Saadat , R. Saadat , and G. Mirjality, "Improving Threshold Assignment for Cluster Head Selection in Hierarchical Wireless Sensor Networks," Proc. of Int'l Symposium on Telecommunications, pp. 409-414, Dec. 2010.

[11] P. Ren, J. Qian, L. Li, Z. Zhao, and X. Li, "Unequal Clustering Scheme based LEACH for Wireless Sensor Networks," Proc. of Fourth Int'l Conf. on Genetic and Evolutionary Computing, pp. 90-93, Dec. 2010.

[12] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method," Scientific World Journal, 2015.

[13] D. Liu, "Resilient Cluster Formation for Sensor Networks," Proc. of 27th Int'l Conf. on Distributed Computing Systems (ICDCS '07), pp.40-48, 2007

[14] K. Sun et al., "Secure Distributed Cluster Formation in Wireless Sensor Networks," Proc. of 22nd Annual Computer Security Applications Conference (ACSAC'06), pp. 131-140, 2006

[15] S. Mayur, H. D. Ranjith, "Security Enhancement on LEACH Protocol From Sybil in WSN Using LDK Scheme," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, ISSN (Online): 2319 – 8753, ISSN (Print): 2347 – 6710, March 2015.

[16] Sweety Saxena and Prof. Vikas Sejwar, " Sybil Attack Detection and Analysis of Energy Consumption in Cluster Based Sensor Networks," International Journal of Grid Distribution Computing Vol. 7, No. 5 (2014), pp. 15- 30, ISSN: 2005-4262.

[17] Dilpreet R. Amuthavalli and R. S. Bhuvaneswaran, " Detection and Prevention of Sybil attack in Wireless Sensor Network Employing Random Password Comparison Method," Journal of Theoretical and Applied Information Technology, September 2014, Vol. 67, No.1, ISSN: 1992- 8645.

[18] V. Sujatha and E. A. Mary Anita, "Detection of Sybil Attack in Wireless Sensor Network," Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 202-206, 2015, ISSN 1990-9233.

[19] G. Wang, D. Kim, and G. Cho, "A Secure Cluster Formation Scheme in Wireless Sensor Networks," Int'l Journal of Distributed Sensor Networks, vol. 2012, Article ID 301750, 14 pages, 2012.

[20] H. Rifà-Pous and J. Herrera-Joancomartí, "A Fair and Secure Cluster Formation Process for Ad Hoc Networks," Wireless Communications, Vol. 56, No. 3, pp. 625-636, 2011.

[21] G. V. Crosby and N. Pissinou, "Cluster-based Reputation and Trust for Wireless Sensor Networks," Proc. of the 4th IEEE Consumer Communications and Networking Conference (CCNC '07), pp. 604-608, 2007.

[22] L. Buttyan and T. Holczer, "Private Cluster Head Election in Wireless Sensor Networks," Proc. of the Fifth IEEE Int'l Workshop on Wireless and Sensor Network Security (WSN '09), IEEE, pp. 1048-1053, 2009.

[23] A. Babu Karuppiah and A. Raja Prakash, "SYBILSECURE: an energy efficient sybil attack detection technique in wireless sensor network," International Journal of Information Sciences and Techniques (IJIST) Vol. 4, No. 3, May 2014.

[24] M. Sirivianos et al., "Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," Proc. of Int'l Sympo. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '07), Cyprus, pp. 1-10, Apr. 2007

[25] Q. Dong and D. Liu, "Resilient Cluster Leader Election for Wireless Sensor Networks," Proc. of IEEE 6th Annual Comm. Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks(SECON), pp108-116, 2009.

[26] I. Nishimura, T. Nagase, Y. Takehana, and Y. Yoshioka, "Secure Clustering for Building Certificate Mangement Nodes in Ad-Hoc Networks," Proc. of 14th Int'l Conf. On Network-Based Information Systems (NBiS), Tirana, Albania, Sep. 07-09, 2011

[27] J. Steffi, Agino Priyanka, S. Tephillah, and A. M. Balamurugan, "Attacks and countermeasures in WSN," International Journal of Electronics & Communication, Volume 2, Issue 1, ISSN 23215984, January 2014.

[28] R. Amuthavalli & R. S. Bhuvaneswaran , " Genetic Algorithm Enabled Prevention of Sybil Attacks for LEACH-E," Modern Applied Science; Vol. 9, No. 9; 2015, ISSN 1913-1844 E-ISSN 1913-1852.

[29] Reza Rafeh and Mozhgan Khodadadi , " Detecting Sybil Nodes in Wireless Sensor Networks using Two-hop Messages," Indian Journal of Science and Technology, Vol. 7 (9), 1359–1368, September 2014, ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645.

[30] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE journal on selected areas in communications, Vol. 29, No. 3, March 2011.

[31] Nusrat Fatema, Remus Brad, "Attacks and counterattacks on wireless sensor networks," International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 4, No. 6. December 2013.

[32] A. Anup wanjari, Vidya Dhamdhere, "Evading Flooding Attack in MANET Using Node Authentication," International Journal of Science and Research (IJSR), Volume 3, Issue 12, ISSN (Online): 2319-7064, December 2014.

[33] A. V. Vibi, G. V. Padmasree, P. Nithya, and C. Geetha, "Detection of sybil attack using neighbouring node messanging using wireless sensor network," International Journal of Advanced Technology in Engineering and Science, Volume No. 3, Issue No. 3, March 2015, ISSN (online): 2348 – 7550.

[34] Udaya Suriya Rajkumar and Rajamani Vayanaperumal, "Compare and Match Approach for Preventing Sybil Attacks in Wireless Sensor Networks," International Journal of Engineering Technology Science and Research, Volume 2, Special Issue September 2015, ISSN 2394 –3386.

[35] C. Venkata, Mukesh Singhal, James Royalty, and Srilekha Varanasi, "Security in wireless sensor networks," Wireless communications and mobile computing Published online in Wiley Inder Science, 2006

[36] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trappe, "Channel-Based Detection of Sybil Attacks in Wireless Networks," IEEE Transactions on information forensics and security, Vol. 4, No. 3, September 2009.

[37] A. Hamid, Mamun Rashid, Choong Seon Hong, "Defense against lap-top class attacker in wireless sensor network," The 8th International Conference Advanced Communication Technology, Print ISBN: 89-5519-129-4, IEEE, 2006.

[38] Waldir Ribeiro Pires J´ unior Thiago H. de Paula Figueiredo Hao Chi Wong, "Malicious Node Detection in Wireless Sensor Networks," 18th International Parallel and Distributed Processing Symposium, Print ISBN:0-7695-2132-0, IEEE, 2004.

[39] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN," International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[40] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks," The International Arab Journal of Information Technology, Vol. 9, No. 3. May 2012.