Secure multi-level Cluster based wireless sensor network

Husna Akbar IICT
MUET
Jamshoro, Pakistan
husna09.akbar@gmail.com

Syeda A. Afghan Faculty
of Informatics University
of Debrecen Hungary
adila@eng.unideb.hu

Sana H. Jokhio
Melbourne, Australia
shoorjoks@gmail.com

Imran A. Jokhio School
of IT & Eng. MIT
Melbourne, Australia
ijokhio@mit.edu.au

***Abstract* —The demand of wireless sensor networks (WSNs) is on the raise due to its potential applications. The data transmission occurs via a wireless link by the sensor node in network hence these nodes are vulnerable to several outside or inside attacks. A WSN may works in an unfriendly environment therefore it is a fundamental requirement of WSN to secure the sensing data. In this paper, we focus on highlighting the security issues in a multi-layer WSN architecture and provide a secure communication solution (combination of various state- of-art protocols) for it by considering the WSN constraints. We propose a multi-level protocol distribution method to enhance the security of the WSN under consideration via targeting and providing resilience to specific attacks at each level. The simulation and results show that by implementing our proposed method, the overall security of the network has been enhanced.**

Index Terms—WSN, cluster based routing, security, attacks, vulnerabilities

I. INTRODUCTION

A wireless sensor network is used in various fields such as security and surveillance, environmental monitoring, industrial application, transportation, and health-related areas. Many security protocols have been proposed in the literature to enhance overall security of a WSN. A WSN may use various topologies to communicate the sensed data by the sensor nodes to the base station [1]. WSN is vulnerable to security attacks because of as it uses shared wireless medium which may increase the chance for an adversary to eavesdrop, monitor the network traffic or even get access to the network resources. Hence, the types of attacks that may be carried out by an adversary range from simple eavesdropping to wormhole attacks.

Secure and efficient data transmission is required for a security sensitive application of a WSN that may be deployed under harsh environment. A cluster based network consists of end nodes, cluster heads and a base station (BS). Each cluster contains a group of end nodes and a cluster head (CH). The end nodes detect the phenomenon and report to the CH. The CH processes the collected data and reports to the BS and other cluster heads of the network [3]. Hence, multiple levels of communication may be considered in a cluster based WSN. For securing a network it is always important to identify the security concerns with respect to the type of application prior to deploying the network [2]. These issues may include

• Confidentiality

• Integrity

• Authentication of data in a specific network.

The applications of WSNs are increasing day by day. Various types of network arrangements are used in WSN. We focus on multi-level cluster based network architecture. It is important that the network link be secure enough between source and sink to transmit data fearlessly. It may not be a good idea to use a single type of security mechanism at all the levels of communication in a cluster-based network. Nevertheless, keeping the WSN constraints in mind, the security solution should focus on protecting data at various levels as to strengthen network resilience to various security attacks and to guarantee secure communication at multi-layer. In this paper we highlight the security issues in a multi-layer WSN architecture and provide a secure communication solution (combination of various state-of-art protocols) for it by considering the WSN constraints.

The rest of the paper has been organized as follows. Section

2 presents the related work and detailed literature review regarding cluster based wireless sensor networks, their fundamental properties and various security techniques that are used for secure sensing applications. A brief discussion on globally proposed routing and security protocols for WSN has also been presented. We discuss the bedrock of our proposed security technique in Section 3. A summary of the secure routing protocols considered to be used at multi-level cluster based WSN is presented in this section. Moreover, brief architecture and protocols working have also been discussed. This section also contains study on combining these protocols that may provide better result in securing a WSN and may provide efficient resilience against attacks in WSN. Section 4 contains the Simulation details, analysis and discussion regarding the proposed multi-level secure WSN. This section also contains discussion regarding attacks on WSN and shows simulation results of the proposed work. Section 5 provides conclusion of the research work and discusses future work.

II. RELATED WORK

A number of cryptographic schemes have been proposed globally. Some focus on certain specific types of attacks, others highlight security issues and threats and propose attack resilient options for security sensitive applications of WSNs. However, a number of security challenges are still of research

of a WSN may have a unique deployment or arrangement of sensor nodes in a geographical region. Such arrangements may also impose security risks if the WSN application is se- curity sensitive in nature. We discuss a few globally proposed security solutions of WSN in this section.

G. Padmavathi and D. Shanmugapriya discuss a wide variety of attacks in WSN in [4]. The discussed attacks include attack against privacy, DoS, physical attack, etc. Their classified security mechanisms are also discussed and have been categorized into; Low level security mechanism and the high level mechanism. The lower level mechanism basically focuses on creating a secure connection among the nodes so as to a establish secure communication whereas the high level mechanism is responsible for secure data management and traversing.

M. Chowdhury, et al. in [5] investigated issues and challenges related to WSNs security. The paper described different security threats and attacks, and provided security solution in terms of cryptographic schemes, Key Management Protocols, Secure Data Aggregation, Secure Routing, etc. A thorough review is presented with respect to the globally proposed security mechanisms for WSNs.

S. Ozdemir proposed Secure and Reliable Data Aggregation protocol (SELDA) [6] that integrates secure data aggregation schemes and secure routing. They employ distributed sensor nodes using monitoring schemes to observe misbehaving of sensor nodes. If no intrusion is detected, there is no need to use expensive secure data transmission. To keep a track of their neighbors the proposed monitoring scheme need low- cost sensor nodes to operate in the region. High energy consumption is observed by sensor nodes because the scheme requires the nodes to be up all the time for monitoring.

Sakai et al. in [7] proposed a scheme that is identity-based and uses non-interactive key agreement. This scheme is based on bilinear pairings. All sensor nodes are given a unique ID and mutual secrets that are never disclosed. The two nodes create a cryptographic key that is used to encrypt and decrypt the data communication. Hence this scheme doe not impose a communication overhead on the sensor nodes due to its non-interactive nature. Using the Unique IDs and the secrets, the sensor nodes can communicate over the unsecured wireless medium.

Globally, focus has been put on design and development of efficient routing protocols. And often they are complemented with security to create a secure and efficient routing protocol that may result not only providing secure communication but may overcome some WSN constraints. But in order to design such protocol, it is important to highlight the security issues and risks with respect to a security sensitive application of WSN. WSN Security issues are discussed next.

A. WSN Security Issues

Wireless Communication is used by WSNs to transfer information within the network hence they are vulnerable to those security attacks that may not impose a risk on

the adversary cannot directly tamper the line. However, the securing the communication within the wireless network may be a challenging task as it is carried out via broadcast. During the broadcast the adversaries may launch eavesdrop, inject, intercept and may even alter the data that is being communicated. These adversaries may be operating from a distance and may be highly equipped and sophisticated in nature. Resource consumption attacks can be easily carried out on sensor nodes. The adversaries may keep the nodes busy and as a result the batteries might drain out soon. Bandwidth may be utilized and fake messages may be created to keep the nodes busy.

WSNs are often deployed under harsh environments. These environments are insecure and may lead to node capture and tampering. This may result in an adversary impersonating a legitimate node because if the sensor node is tampered with, it can reveal all the secrets and security information to the adversary. The cluster based network has unique structure in which the sensor (end) nodes are connected to the BS via the CH. While using a single security mechanism may secure the network against some attacks, using more than one secure algorithm might solve bigger issues. Nevertheless, by using appropriate security protocols at specific cluster level, the security of the overall network may be improved. We discuss our proposed method in the next section.

III. LIGHT-WEIGHT MULTI-AGENT ROUTING FRAMEWORK

WSN are often deployed over certain geographical regions where maintenance is a challenging task. Nevertheless, certain WSN applications are security sensitive in nature and to keep the detected phenomenon by the sensor node a secret is fundamental for the lifetime of that network. We discuss our proposed strategic method to secure a multi-level cluster based WSN in this section.

A number of security protocols have been proposed globally that claim a number of properties. If thoroughly observed, it shows that the cluster based network may be divided into different layers. These layers may consist of sensor nodes

with different capabilities. The end nodes, for example, may have low configuration as compared to the cluster head nodes. Hence the communication may be less between a sensor node and the cluster head whereas a cluster head may need to communicate with CHs of other clusters as well as with the base station. Therefore the communication among various nodes may be divided into multiple levels in a cluster based WSN. At times the types of attacks caused by the adversary against a network might vary according to the type of the devices such as End Node (EN), Cluster Head (CH) or Base Station (BS). We consider two levels (as per communication among the nodes) in a cluster based network. The levels are divided as follows:

• Level 1 Communication between EN and CH

• Level 2 Communication among CH to CH and CH to BS

The arrangement of a cluster based WSN varies with respect to geographical arrangement of nodes, nodes duties and their configuration. Using single cryptographic scheme at all the cluster layers might not be able to resist majority of possible attacks by an adversary. A number of protocols were studied and analysed. Three protocols were chosen based on the properties such as light-weight in terms of energy consumption, least processing overhead, light-weight in terms of memory usage, to provide resilience to considered attacks Replay, Sybil and Wormhole attacks.

The selected protocols are Secure Sensor Protocol for Information via Negotiation (SSPIN), Secure Ad hoc on Demand Distance Vector Routing (SAODV) and Energy-Efficient Secure Routing Protocol (EESRP). As the end nodes are less capable as compared to the CHs hence we need a protocol that does not consume too much energy in executing the security protocol and communication. To evaluate security of a network, where we define the capabilities of legitimate sensor nodes, we also define the adversary model or the capabilities. Hence here we are considering that the adversary has similar capabilities as that of an end node. Nevertheless, all attacks cannot be eliminated at all levels. Hence we narrow them down Sybil, Reply and Wormhole attacks. Where Sybil and Replay attacks are considered at level 1 and the wormhole attack is considered at level 2. We briefly discuss the protocols below.

A. SAODV Protocol

The SAODV is the extension of AODV routing protocol by considering security for the WSN network. The proto- col secures the route discovery and may eliminate security risks involved in authentication, integrity, and non-repudiation. SAODV is claimed to provide resilience against impersonation, black hole and gray hole attacks. It uses two mechanisms to secure messages; Digital Signature to validate the non-mutable parts of the messages, and Hash Function used to provide security to the hop count information [8].

B. SSPIN Protocol

It is a secure extension of SPIN protocol. SPIN design is based on the idea that the sensor nodes send meta-data before sending the actual data for negotiation with neighbors to conserve energy and to work more efficiently. SSPIN uses three types of messages like SPIN to perform a negotiation process between the sensor nodes. These messages types are advertise message (ADV), request message (REQ), and DATA. In addition, a Message Authentication Code (MAC) is also used by SSPIN to protect ADV and REQ messages and it also guarantees the packet correctness and integrity of messages. SSPIN is claimed to protect against security attacks such as replication attack and replayed attacks [9]

C. EESRP Protocol

It efficiently secures the traveling of data packets throughout the route from source node to the sink node. It also consumes less energy as compared to other protocols by distributing the network load evenly among the sensors. This may also increase the lifetime of the network. It has been developed using two protocols; Roulette-Wheel Routing Protocol (RWRP) and Secure Routing Protocol (SRP) [10]. Apart from providing resilience to a number of security attacks, EESRP protects the network against wormhole and sinkhole attacks.

In a cluster based network, using single security scheme in routing data over the network may not provide resilience to most security attacks. While using different security protocols at multi-levels of cluster based network may provide protection against efficient number of WSN attacks. We discuss our simulation results in the next section.

IV. SIMULATION AND RESULTS

Using a single protocol to secure a cluster based WSN may not provide resistance to majority of attacks carried out by an adversary. We discuss the simulation results in this section and provide a thorough security analysis regarding our proposed solution.The simulation is initially carried out to evaluate the claimed advantages of the selected protocol and to find out which of these protocols might work better on which layer of the cluster based WSN. The cluster based WSN has been divided into two levels. Different levels might require different level of security with respect to the configuration or the capabilities of the nodes at that level.

A. Scenarios

Network Simulator (NS) was used to simulate the proposed

scenarios and to evaluate the results. Two scenarios were simulated. Overall performance of the protocols was evaluated not only with respect to the security but also with respect to the burden it may put on the sensor node considering the WSN constraints such as memory, processing and energy consumption. The scenarios are further discussed below.

1) SCENARIO 1: : In this scenario an individual protocol was used to secure the entire cluster based WSN (all the levels). This scenario highlighted the strengths and weaknesses of the protocol with respect to varying capabilities of the sensor nodes and the adversary. So the communication occurs between end node to cluster-head, cluster-head to cluster-head and cluster-head to base station. The considered security attacks in this scenario are Eavesdropping, Replay, Sybil and Wormhole attacks. The adversary has been modeled to be possessing similar capabilities as that of an end node. Figure

1 shows screen shot of the simulated scenario 1.

2) SCENARIO 2: In this scenario we divide the communi-cation into two levels i.e. cluster level 1 and cluster level 2 as shown in Figure 2 below.

• CLUSTER LEVEL-1: At level 1, the communication occurs between end-nodes and cluster-head only. Due to the limited capabilities of an end node in cluster level

1 the selected security scheme must be light-weight in terms of energy consummation of sensor node. More- over, it should not impose an overhead with respect to memory and computation or processing. The adversary model considered at this level has similar capabilities as

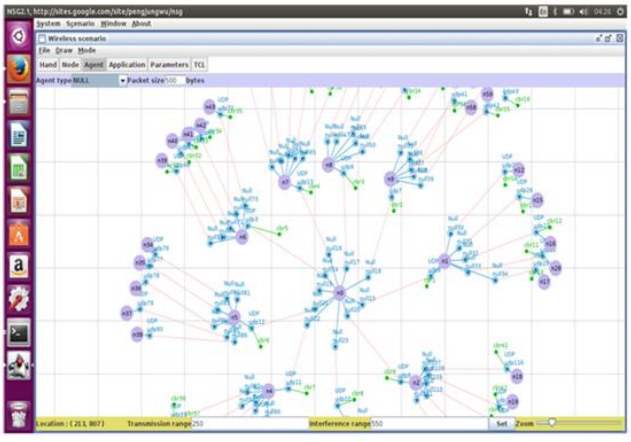

Fig. 1. Scenario 1 Nodes Arrangement

that of an end node. Considered attacks on nodes are Eavesdropping, Replay and Sybil. Considered protocols for this level are SAODV and SSPIN.

• CLUSTER LEVEL-2: At level 2 the considered com-munication occurs between cluster-head to cluster-head and cluster-head to base station. As capabilities of a cluster-head may be more as compared to those of an end node hence it is possible to use a security scheme which may have communication or processing overhead. The Adversary has the same capabilities as that of a cluster- head node. Considered attacks on nodes is the wormhole attack. The considered protocol for this level is EESRP only.

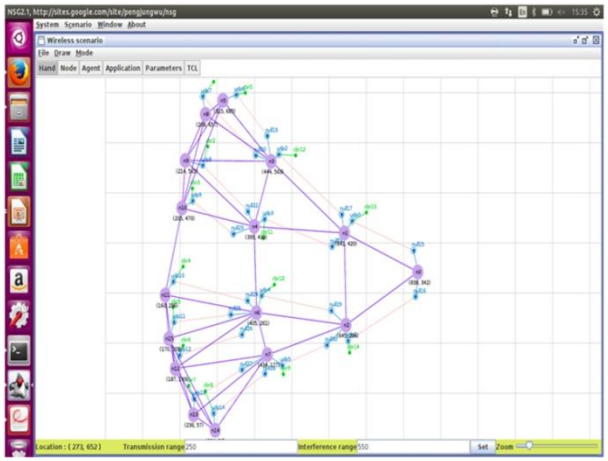

Fig. 2. Scenario 2 Nodes Arrangement

B. Overhead Evaluation

The selected protocols were initially evaluated for the overhead they may impose on a sensor node in terms of memory utilization, processing of the protocol and the overall energy consumption. It is important to know which protocol might impose, an overall, less overhead in terms of the above mentioned parameters to be able to use at a specific level of the cluster based WSN. The results are discussed below.

the designed security protocol should impose less memory overhead for the sensor to work without interruptions and delays. The figure 3 below illustrates the memory overhead each protocol imposes on a sensor node, especially the end node. The graph shows that SSPIN is light weight in terms of memory usage as compared to SAODV and EESRP. Hence, based on the findings SSPIN may help in securing the sensor node at a specific level of the cluster based network along with increasing the overall life time of the node The design of

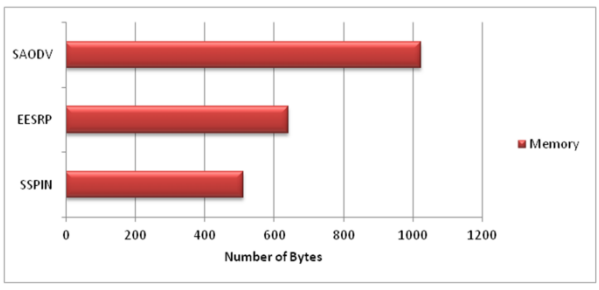

Fig. 3. Memory Utilization of a Sensor Node by each Protocol

a protocol should consider least energy consumption as it is

one of the most important constraints of the WSN. Securing a network may involve a number of routines to be executed resulting in an increase in the energy consumption of the sensor node involved. This may result in a decrease in the overall life time of the sensor node. The selected protocols were simulated and the results were analyzed with respect to the energy consumed by each protocol while they were executed. Each node was assumed to possess 32400 Joules of energy that is equivalent to the one produced by two AA size batteries. The assumption is based on the fact that each sensor node may be operated by 2 AA batteries in a real time WSN application. So all nodes have 32000 joules at the time of deployment then it reduces with time and communication of detected data. Here again the SSPIN consumption is better as it has so far consumed less energy. Residual energy in a node that used SSPIN is higher than others. The figure 4 below illustrates the energy consumption by each protocol. SSPIN again seems to be the winner with EESRP being the runner up. Hence, SSPIN may be used to secure the level 1 of the cluster based WSN. Heavy instruction or information processing by a sensor

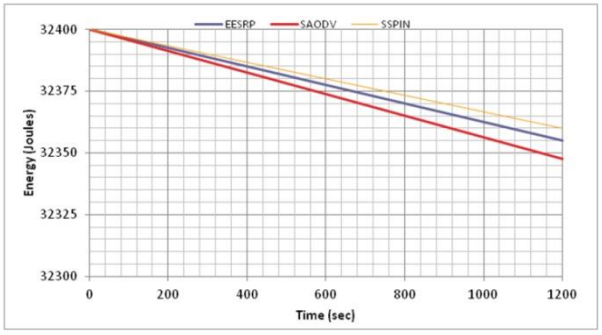

Fig. 4. Energy Consumed by a Sensor Node during protocol execution

node may result in more energy consumption and/or memory utilization. Hence a protocol that is light weight in terms of processing or in other words requires less processing may be a good choice to use at the lower level of a cluster based WSN. The figure 5 below shows that the overall processing overhead by the three selected protocols. This graph actually hows the time to process the security mechanism by sensor node. Again SSPIN is the winner. SSPIN has less processing time as compared to that of SAODV and EESRP. SAODV takes more time to process because it uses two security mechanisms; the digital signature and the hash function. However, EESRP has moderate processing time as it uses two protocols; one is responsible for taking route decision while the other for securing the network. These results helped in selecting the

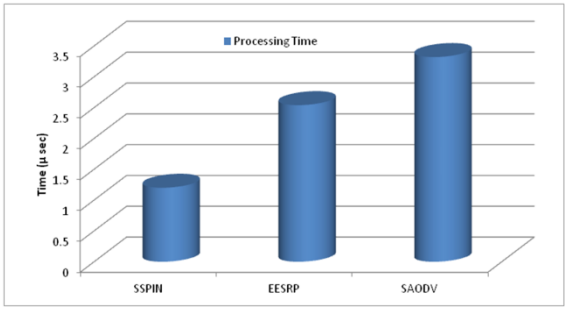

Fig. 5. Processing Time of each Protocol

protocols that may be suitable to secure a specific level of a cluster based WSN as every level has sensor nodes with different configuration and/or capabilities. We now evaluate the security of these protocols to verify the types of attacks these may provide resistance to. The findings are discussed below.

C. Security Analysis

The selected protocols, SAODV, SSPIN and EESRP were simulated via two scenarios and were tested against security attacks to evaluate their strengths and weaknesses in terms of their resistance to specific attacks. Detailed analysis and discussion are available below.

1) Replay Attack: Considering the network has one node

act as a malicious node. The attack resistance of the protocols was evaluated. The capabilities of the malicious node are that of the legitimate node under consideration (for example, if an end node is under attack, the adversary has similar configuration as that of an end node). The attack resilience of two protocols, SAODV and SSPIN was tested against Replay attacks. These protocols were claimed to have been providing resistance to such type of attack. The considered adversary for the attacker model was assumed to have similar capabilities as that of an end node. The figures 6 and 7 below show the simulation results for the Replay attacks detected by SAODV and SSPIN. SAODV performs badly as the number of attacks detected by it is less. Red shows attacks and blue shows how many were actually detected. Approximately 60% of the attacks were detected which is not good enough for a security

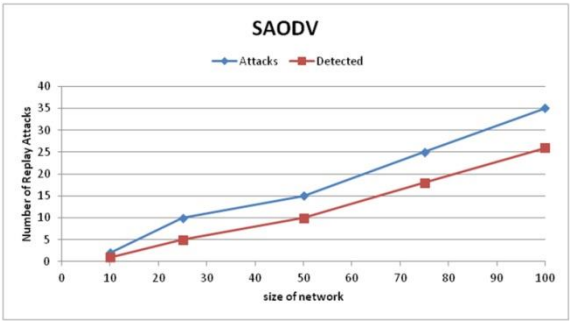

Fig. 6. Replay Attacks detected by SAODV Protocol

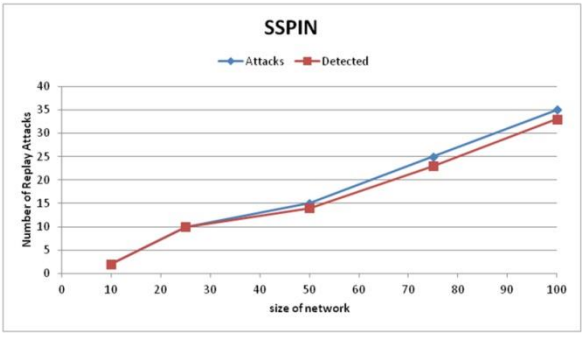

Fig. 7. Replay Attacks detected by SSPIN Protocol

sensitive application as this is a very simple form of attack. Whereas, SSPIN performs better and detects most of them. Hence, it may be used to protect a lower cluster level in a cluster based WSN.

2) Sybil Attacks: In a replay attack, the attacker eavesdrop the conversation of two legitimate nodes and then might just replay the message to another node to misguide. This is the simplest type of attack that can be carried out after just simple eavesdropping. One attacker can only impersonate the sender or the receiver whereas, in a Sybil attack, the attacker can impersonate both the sender and the receiver simultaneously to misguide other nodes. This type of attack can be carried out by an adversary that may or may not possess better capabilities than the attacked node. Hence here we consider the adversary with similar capabilities as that of a legitimate node. This attack is difficult to detect because in this attack the attacker node has more than one identity. Figures below illustrate the simulation results for this type of attack while using SAODV and SSPIN to protect the cluster based WSN.

SAODV performs badly it does not detect attacks (Figure 8). The gap between the lines is more which shows the protocol performs badly. SSPIN is the winner here too as it detects almost all Sybil attacks (Figure 9).

3) Wormhole Attacks: Two attackers are used in this attack whereas a single attacker may carryout Replay and Sybil. Wormhole attack is a sophisticated one as in this attack the attacker creates a secret link and communicates the information with the second attacker. This type of attack can bring more harm to the network. SAODV and SSPIN do not provide

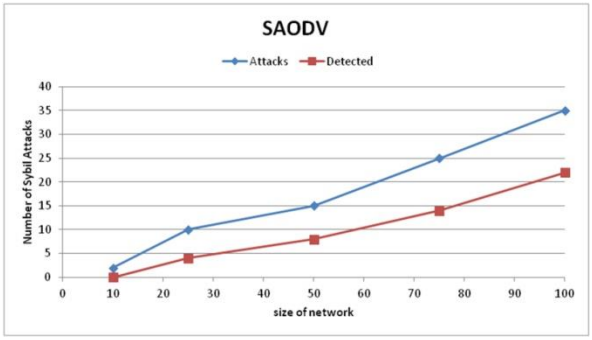

Fig. 8. Sybil Attacks detected by SAODV Protocol

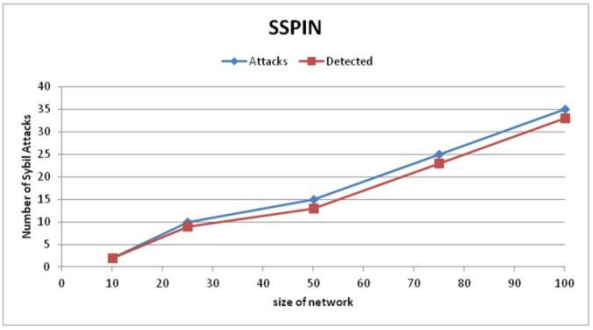

Fig. 9. Sybil Attacks detected by SSPIN Protocol

the resistance to wormhole attack (as per literature review)

hence only EESRP protocol has been considered. The figure

10 below shows EESRP provides satisfactory resilience to the wormhole attacks. Being sophisticated in nature, it is difficult

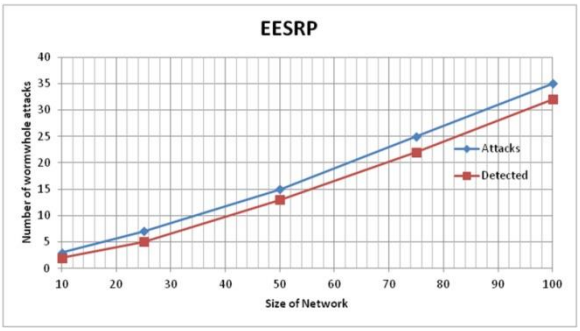

Fig. 10. Wormhole Attacks detected by EESRP Protocol

for any protocol to detect the wormhole attack. But EESRP performs satisfactorily hence if considered, it may be used to protect the level 2 (communication between CH to CH and CH to BS). Nevertheless, the adversary that carries out a wormhole attack is considered to be more sophisticated and possesses better capabilities. As CH are considered more capable than end nodes, the EESRP protocol implementation at level 2 may actually help in securing the network against more powerful attacks.

The overall results illustrate that verifying the imposed overhead by the selected protocols may actually help in selecting specific protocol for a specific cluster level communication.

Moreover, each protocol was evaluated to determine the degree to which they may provide resilience to various security attacks. We conclude our findings in the next section.

V. CONCLUSION

In this paper we present secure multi level cluster based WSN method. This method incorporates the state of art pro- tocols SAODV, SSPIN and EESRP security protocols which have

been discussed and simulated. By using a multi-layer approach in a cluster based WSN the simulation results show that overall attack resilience of the WSN has improved. At each selected level (independently) the overall processing and memory overhead was reduced. The simulated cluster based WSN using the selected security protocols could resist replay attack, Sybil attack and wormhole attacks successfully. EESRP and SSPIN protocols give satisfactory results in the protection of WSN network from attacks. SAODV alone does not provide resistance to wormhole attacks. Nevertheless, performance of SAODV is not satisfactory while the WSN is under Sybil or Replay attack. In order to complement present research, the following additional work is suggested:

• The performance of EESRP and SSPIN may be analysed with respect to large scale WSN.

• Other claimed light-weight and secure protocols may be analysed and tested.

REFERENCES

[1] Zeb, A.; Islam, A.K.M.M.; Komaki, S.; Baharun, S., "Multi-nodes joining for dynamic cluster-based Wireless Sensor Network," in Informatics, Electronics and Vision (ICIEV), 2014 International Conference on , vol., no., pp.1-6, 23-24 May 2014.

[2] Prasath, K.A.; Shankar, T., "RMCHS: Ridge method based cluster head selection for energy efficient clustering hierarchy protocol in WSN," in Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on , vol., no., pp.64-70, 6-8 May 2015.

[3] Roy, S.; Kumar Das, A., "Energy efficient cluster based routing pro- tocol (EECBRP) for Wireless Sensor Network," in Networks and Soft Computing (ICNSC), 2014 First International Conference on , vol., no., pp.25-29, 19-20 Aug. 2014

[4] Padmavathi G.; Shanmugapriya, D. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[5] Chowdhury M., Kader M. F., and Asaduzzaman A Survey on Security Issues in Wireless Sensor Networks International Journal of Future Generation Communication and Networking Vol.6, No.5 (2013).

[6] 21. Ozdemir, S., Secure and reliable data aggregation for wireless sensor networks, In Ubiquitous Computing System; Ichikawa, H., Cho, W.-D., Sato, I., Hee, Y.Y., Eds; Springer: Berlin/Heidelberg, Germany, 2007; pp. 102109.

[7] 22. Sakai, R.; Ohgishi, K.; Kasahara, M. Cryptosystems based on pairing. In Proceedings of the SCIS2000-C20, Okinawa, Japan, 2628 January 2000.

[8] Chakraborty, S.; Khan, A.K., "A noble approach for self learning and cluster based routing protocol with power efficiency in WSN," in Communications and Signal Processing (ICCSP), 2014 International Conference on , vol., no., pp.773-777, 3-5 April 2014.

[9] Tang, L.; Li, Q. S-SPIN: A Provably Secure Routing Protocol for Wireless Sensor Networks. International Conference on Communication Software and Networks, IEEE Computer Society 2009.

[10] El-Semary, A. M. Energy-efficient secure routing protocol based on rulette-wheel and TESLA for wireless sensor networks. The Interna- tional Journal of Sensor Networks and Data Communications, vol.1, ArticleIDX110201,13 pages,2012.