Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 12, December 2018, pg.291 – 303

Trust Based Approaches to Counter Selective Attacks on Wireless Sensor Networks

Jeelani[1], Manoj Rana[2], Subodh Kumar[2], Aasim Zafar[3]

[1,2]Department of Computer Application, IET, Mangalayatan University, Aligarh, India
E-mail: jeelani.0018@gmail.com [1], manoj.rana@mangalayatan.edu.in [2], subodhkumar.86@gmail.com [2]
[3]Department of Computer Science, Aligarh Muslim University, Aligarh, India
E-mail: aasimzafar@gmail.com [3]

Abstract-- Wireless sensor networks (WSN) has a growing prospect because of its low-cost, power-efficient, and easy-to-implement characteristics. However, its security problems have become hot topic of research nowadays. Selective attacks are just one of frequently encountered security problems, which are easily combined with other attacks to cause more damage to the network. In this paper, the authors discuss trust based approaches to counter selective attacks, namely, Sybil, Wormhole, Black-hole, Gray-hole, Hello flood, and Distributed Denial of Service attacks on wireless sensor network WSNs. The countermeasures are not only capable of detecting compromised sensor nodes vulnerable for selective attacks but also detect all compromised messages transmitted to the base station through the sender nodes.

Keywords— Wireless Sensor Networks (WSN); Trust; Countermeasure; Distributed Denial of service (DDoS); Wormhole attack and so no

I. INTRODUCTION

Wireless sensor networks (WSN) are a multi-hop temporary autonomous system made up of a group of mobile nodes with wireless transmitters and receivers. Not relying on any preset infrastructure, it would achieve automatic organization and running in arbitrary Mesh topology. Together with micro-processing and wireless communication capabilities, they are widely used on occasions which require rapid deployment and dynamic networking, such as military tactical communications and emergency communications [1, 21]. They are becoming a hot research subject of critical significance in many practical applications. However, wireless sensor networks are vulnerable to various types of attacks, including Sybil, Wormhole, Black-hole, Gray-hole, Hello Flood, and Distributed Denial of Service attacks, which are mainly discussed in this paper and are relatively important attacks.

A more and serious issue is that nodes may be compromised and perform malicious attacks such as packet dropping or packet modifications to disrupt normal operations of a Wireless Sensor Network, where in Sensor Nodes (SNs)

---

[1]Corresponding author: Jeelani (e-mail- Jeelani.0018@gmail.com)

© 2018, IJCSMC All Rights Reserved

usually perform unattended operations. A large number of SNs deployed in the WSN also require a scalable algorithm for highly reconfigurable communication operations. In this paper, we propose trust based approaches to counter the earlier mentioned selective attacks on wireless sensor networks.

The present manuscript has been structured as follows: Section II lists the common attacks on Mobile Ad-hoc Network (MANET) and in WSN. Section III presents the trust and system model, while related work is discussed in Section IV. Selective attacks and its countermeasures are given in Section V. Finally, we conclude the paper in Section VI.

II. ATTACKS ON MOBILE AD-HOC NETWORK (MANET) AND IN WSN

This section deals with the study of comparison of possible attacks on Mobile Ad-hoc Networks (MANETs) and Wireless Sensor Networks (WSNs). Further, we discuss similar attacks on MANETs and WSNs.

A. Common Attacks

Here are common attacks of Mobile Ad-hoc Network MANET and Wireless Sensor Networks WSNs shown the table I.

TABLE I: LIST OF COMMON MANET AND WSN ATTACKS.

Attacks on MANETs	**Attacks on WSN**
Sybil Attack	Sybil Attack
Wormhole Attack	Wormhole Attack
Black-hole Attack	Black-hole Attack
Gray-hole Attack	Gray-hole Attack
Hello Flood Attack	Hello Flood Attack
Distributed Denial of Service Attack	Distributed Denial of Service Attack
Replay Attack	Replay Attack
Byzantine Attack	Byzantine Attack
Blackmail Attack	Jamming Attack
	Collision Attack
	Sinkhole Attack
	Selective Forwarding Attack
	Clone Attack
	Information Forwarding Attack

B. selective similar attacks both in MANET and WSN

Some Selective Similar attacks in MANET and WSNs are as given below in table 2.

TABLE 2: SIMILAR ATTACKS IN MANET AND WSNS.

Similar attacks in MANET and WSNs.
Sybil Attack
Wormhole Attack
Black-hole Attack
Gray-hole Attack
Hello Flood Attack
Distributed Denial of Service Attack

These are most common type of attacks; and hence, we shall focus on these selective attacks only in this study.

© 2018, IJCSMC All Rights Reserved

III. OVERVIEW OF TRUST AND SYSTEM MODEL

In this section, we discuss about trust and system model and their interconnection with WSN.

A. TRUST

As one human can trust on some other human based on his history of behavior with that person and by identifying the abilities that particular person is capable to handle if given certain task, in same manner one sensor node can set up a trust on some other sensor node based on past communications with that node and the capabilities of that particular sensor node to perform certain task. Capability of sensor node can be identified by various factors such as amount of energy remained, amount of memory space that it has to perform certain networking task, etc. [17].

In the present study, we will identify various trust factors that one node can use to evaluate the trust of another node to decide whether particular node is trustworthy or not. Trust in WSN can be viewed as communication trust and data trust or node trust, path (connectivity) trust and service trust, energy trust, honesty, task completion capability, reliability, familiarity and so on. The trust is non-transitive, subjective, symmetric and reflexive in nature [5]. If there rules of networking are properly followed, while nodes are performing action then trust between nodes increases. If these node don't follow the rules properly then these nodes are considered a malicious and they are ignored from further networking tasks. One node can build a trust about other nodes based on past communication behaviors, energy level that particular node has and by getting recommendations from some other nodes about the node for which trust is to be established.

Many researchers have proposed trust based models [6] by considering either one of the trust factor such as communication trust or data trust. But most of trust models are not considering the other factors that can influence the trust of sensor node. So it is always important to consider all factors to design Intrusion Detection System (IDS) that will be able to detect wide range of malicious behaviors in WSN based on trust of sensor nodes. As of today there is very few study done in this direction to propose IDS by considering trust of sensor node to detect malicious and selfish nodes. We hope and believe our Intrusion Detection System will be first to include all such aspects of trustworthiness to detect malicious nodes in wireless sensor network.

B. SYSTEM MODEL

Here we consider all sensor nodes are randomly placed that are unable to move from their locations. We consider nodes in network to be of one of the kind either subject node, object node, recommender as shown in Fig.1. The node which wants to obtain trust value of another node is called as Subject node, evaluated node is known as Object node and apart from that if we consider a cluster based WSN, then there is a special kind of node called Cluster head which is selected based on nodes characteristic. Generally, the node which is having more energy and more memory to perform various networking operations is considered is selected as Cluster head. Cluster head can evaluate trust of all sensor nodes in its cluster to detect whether there is any malicious node in cluster so as to ignore that node from further intra-cluster operations.

Trust can be evaluated between two senor nodes or between cluster head and sensor node. If we observe a big picture, then one cluster head can also evaluate trust of some other cluster head in the network. Here in this paper, we consider cluster heads also as one of the sensor node and we will try to establish IDS in which every node is able to evaluate any other node irrespective of whether it is cluster head or sensor node.

C. TRUST BASED INTRUSION DETECTION

Trust based Intrusion Detection (TBID) model not only evaluates communication behavior to establish trust, but also examine all the factors for formation of Trust. There are various kinds of trust that can be established between two sensor nodes depending on whether these two nodes are considering the direct communication behaviors or taking help of some other node to establish a trust. We basically classify the trust among following categories [18].

a. Classification of Trust

i. **Direct Trust:** This trust reflects the trust relationship between two neighbor nodes. It is calculated based on direct observation of communication behaviors among two sensor nodes [7].

© 2018, IJCSMC All Rights Reserved

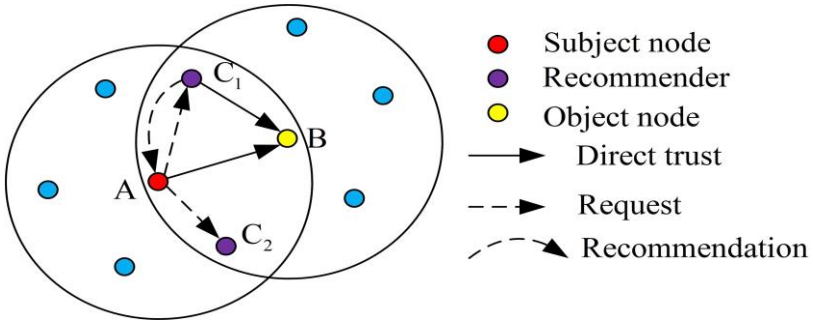

Figure 1: System Architecture.

ii. **Recommendation Trust:** Most of the time a particular sensor node's behavior is well with particular node for some time, at that time it is important to take recommendation about that node from some other third party. The trust derived from third party about object node is called a recommendation trust and third par party is called a recommender.

iii. **Indirect Trust:** Whenever subject node cannot directly observe the communication behavior of object node, indirect trust is established. To establish indirect trust, it is important to get the recommendation values from other nodes.

iv. **Quality of Service Trust:** Node will be judged based on the quality of service that particular node is providing to its neighbors. There are various parameters that can identify the quality of sensor node such as task completion capability, cooperativeness, etc.

v. **Social Trust:** Social trust in WSN may include honesty, communication behavior (intimacy), privacy centrality and connectivity.

Out of these trust identified we are going to believe direct trust, recommendation trust and indirect trust to evaluate the trustworthiness of sensor node in our TBID model.

b. Calculation of Subjective Trust

Subjective trust of sensor node will be calculated based on direct trust, recommendation trust and indirect trust of sensor node. Subjective trust is going to be updated after a period of time and is compared with objective trust which is calculated based on the actual information of each node without considering any network dynamics such as node mobility, trust decay over time, and any malicious attacks.

Subjective trust $T_t^{subjective}$ of sensor node at time t is calculated in the following way:

$$T_t^{subjective} = W_D + T_D + W_R T_{rel} + W_1 + T_{indi}$$

where, T_D, $T_{relibility}$ and T_{indi} are the direct trust, reliability of recommendation and indirect trust of sensor node. WD, WR and W1 are the weights associated with direct trust, recommendation trust and indirect trust respectively such that WD + WR + W1 = 1, and each weight varies from 0 to l depending on whether subject node and object node are one hop neighbor or multi-hop neighbor. If two nodes are able to directly establish trust then weight value WD = 1 and recommendation trust and indirect trust will not be considered as WR = Wt = 0; sometimes even though two nodes are one hop neighbor subject node can take recommendation of object node from other node at that time weight values are distributed among WD and WR. if two nodes are not able to communicate directly then whole weight is given to Indirect trust.

IV. RELATED WORKS

Singh et at. [1] have proposed defense against Sybil attack with the help of a trust based technique TBID (Trust Based Identity Detection) in WSN. The suggested scheme is based on calculating trust values of adjacent sensor nodes. Sing et al. [3] have presented the Sybil attack countermeasures in wireless sensor networks. Dwivedi, et al. [5] have presented various wormhole attack models and different modes of wormhole attacks are also discussed in the paper. Aldhobaiban et al. [6] have proposed a novel way and developed a mechanism to prevent wormhole attacks by an algorithm to manage large number of nodes using node ID called Black-Hole (B-H) attack. Sen et al. [8] have discussed the inherent trust relationship among the nodes in a MANET by formulating a trust model to recognize the trustworthiness of a node. This trust model constructs use of intrusion detection to detect, identify and reduce Black hole attacks. Abd-El-Azim et al. [9] have proposed optimized fuzzy based intrusion detection system

© 2018, IJCSMC All Rights Reserved

is presented with an automation process of producing a fuzzy system by using an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the initialization of the FIS and then optimize this initialized system by using Genetic Algorithm (GA). Alsumayt et al. [10] have given a novel method to detect Denial of Service (DoS) attacks immediately prior to the merger of two MANETs and demonstrated the applicability of the proposed approach in a Grayhole attack, a type of DoS attack. Rose et al. [11] have proposed new technique based on clustering approach and timestamp which is includes two main contributions. One is based on the grouping of sensor nodes and the other is based on the timestamp calculated for one node to another node. Bhuvaneswari and Ramachandran [12] have presented the implementation of ECC algorithm in the prevention of Denial of Service (DoS) attack through fictitious node. Tripathi et al. [13] have provided an overview of LEACH, the most popular clustered routing protocol of WSN and how LEACH can be compromised by Black hole and Gray Hole attacker. Shahabi et al. [14] have suggested a new algorithm which enhances the security of AODV routing protocol to encounter the black hole attacks. This algorithm tried to identify malicious nodes according to nodes' behaviors in an Ad Hoc network and delete them from routing. Tiwari et al. [15] have investigated and a new secure routing technique is proposed for securing the data transmitted over the network. For providing the security a Trust and Opinion based approach is employed on network. Abidoye and Obagbuwa [16] have proposed a message analyser scheme (MAS) for WSNs. The method si capable of detecting compromised SNs vulnerable to a DDoS attack. Duan et al. [19] have proposed a trust-aware secure routing framework (TSRF) with the characteristics of lightweight and high ability to resist various attacks. To meet the security requirements of routing protocols in WSNs, they first analyzed features of common attacks on trust-aware routing schemes. Ozcelik et al. [22] have proposed a novel hybrid IDS for clustered based WSNs by combining the "signature based approach" and "functional reputation based data aggregation and transmission method". Instead of detecting the attacks only in the node level, they suggested a centralized and cooperative scheme using mutual trust evaluations between all network components.

V. SELECTIVE ATTACKS AND ITS COUNTERMEASURES

We put forward here several attacks, like, Sybil attack, Wormhole attack, Black-hole attack, Gray-hole attack, and so forth and its countermeasures [1].

A. SYBIL ATTACK AND TRUST BASED SYSTEMS

Varieties of attacks are possible in WSNs and Sybil is one of them, in which a malicious node illegitimately takes multiple identities. Sybil attack can result in badly determining the routing in the sensor networks. A large number of network security schemes are available for the protection of WSNs from Sybil attack [1].

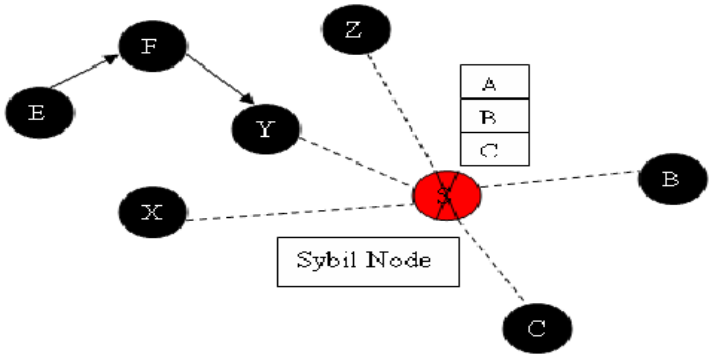

Figure 2: Sybil Attack.

For detecting a Sybil attack, it is prerequisite to recognize the ways in which the network is attacked. This attack is divided into following three categories:

A). Direct and Indirect Communication

i. Direct Sybil attack- The legal nodes communicate openly with the Sybil nodes in the network.

ii. Indirect Sybil attack- This communication is done with the help of malicious nodes.

B). Fabricated and stolen identities

i. Fabricated identities Sybil attack- A malicious node constructs a new identity for itself. This new identity is based on the identities of the legitimate nodes. The method when these malicious nodes communicate with their next

© 2018, IJCSMC All Rights Reserved

neighboring nodes, they build use of any one of fake identities. This result in confusion in the network and it may fall down the entire network.

ii. Stolen identities Sybil attack- The attacker first identifies legitimate existing identities and stole it. This type of Sybil attack will go unidentified in the network in the case of destroying of the node whose identity has been stolen. Node identity replication is completed in the case when the same identities are used for a number of times in the same places in the sensor network.

C). Simultaneous and Non-simultaneous attack

i. Simultaneous Sybil attack- All the Sybil identities participate simultaneously in the sensor network. Due to one identity appearing at a time, looping through the identities will make it to appear at the same time.

ii. Non-simultaneous Sybil attack- The number of identities that are used by assailant is equal to the quantity of physical devices that are present, where each of the devices presents dissimilar identities at different times.

B. SYBIL ATTACK COUNTERMESURES

We shall discuss the best two countermeasures for this attack, namely, SYBILSECURE technique and Genetic algorithm.

i. SYBILSECURE technique

An energy efficient algorithm named Sybilsecure is proposed in [3]. According to the authors, experimental results show that Sybilsecure consumes less energy as compare to the existing defense mechanisms. Sybilsecure is based on sending and acknowledging the query data packets. Social network based schemes that are involved in random routes of data consume more energy in order to detect a sybil node. But in Sybilsecure, less energy is used for detection of sybil node. The planned solution is basically based on sending to and responding from the doubt sent by the cluster head. The Cluster head has a list of its sub nodes parameters, these parameters are identities and their locations. The Cluster head broadcasts query packet to all sub-nodes in such a way that it expects a reply from all the sub nodes, so that they must send their id and location.

ii. Genetic algorithm

Researchers aimed to select nodes for clustering using LEACH-EGA in [3]. This is done in order to improve the energy efficiency with trusted nodes. Before, the clustering in the sensor network, all the nodes are optimized with the help of Genetic algorithm. LEACH-E is used for clustering and CH election. The nodes are advanced with the assistance of characteristics, for example, vitality esteem, trust esteem, remove and so on. As indicated by creators, from the exploratory outcomes, unmistakably the proposed LEACH-E-GA is productive regarding vitality sparing and security. This calculation gives increasingly powerful yield as demonstrated from the charts and tables in the paper. The bundle misfortune is likewise lessened in the proposed methodology by utilizing Genetic algorithm. This empowers the sensor system to proceed with their transmission immediately and dread of attack.

C. WORMHOLE ATTACK

Wormhole attack is a link directly between two malicious nodes. This connection can be wired or wireless with high recurrence and structures a passage which is utilized to pass the information bundle by giving a false course with least bounce warning to the nodes close to its range. At the point when the bundles are sent between the vindictive passages, they are either dropped in the middle of or communicated locally with the goal that it can't reach to its real goal. It is an inactive assault which does not require any data about the information so cryptography can't anchor the information in this attack [4, 5, 6].

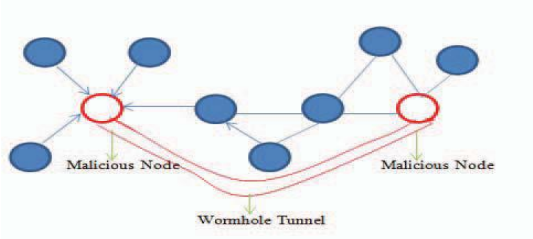

Figure 3: Wormhole Attack.

© 2018, IJCSMC All Rights Reserved

D. WORMHOLE ATTACK MODEL

Wormhole attack models are of basically three types as shown in the figure given below.

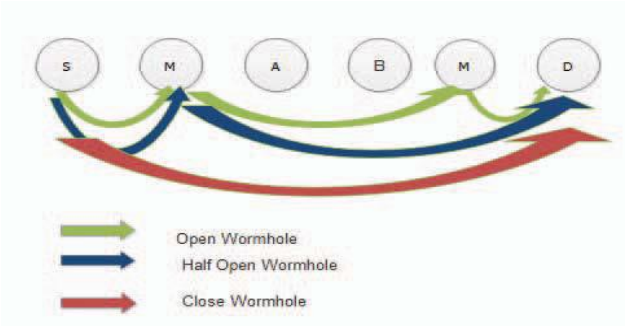

Figure 4: Wormhole attack model.

i. Open Wormhole

Open wormhole is a type of wormhole in which attacker nodes are included in the route discovery process. Other legitimate nodes in between A and B are hidden. The other nodes have illusion that malicious nodes are their direct neighbors.

ii. Half Open Wormhole

In this wormhole, the malicious node close S is unmistakable, yet the malicious node close D is covered up and a passage is made among S and D. There is no malicious action with the bundle on opposite side of wormhole connect. In the root revelation process, just a single side of connection alters the parcel.

iii. Close Wormhole

In close wormhole, all the nodes between source and destination are hidden and a virtual route is created between S and D which gives false information that source and destination are one hop neighbors.

E. WORMHOLE ATTACK COUNTERMESURES

This work is based on the countermeasures of wormhole attack in a particular network. In this article, a detection and prevention (countermeasures) mechanism is proposed securing the communications between source and destination node. While sensor node wants to start communication, the first thing it does is a neighbor discovery from the neighbor list. It generates an encrypted flare message with a top secret key. As soon as the neighboring node receives this beacon frame, it will be decrypted and the acknowledgement route reply (RREP) is sent back to the sender [5].

The following steps will verify a neighboring node in the network.

Data: Given- Network N with node radius r, nodes n and m are nearest neighbors, wormhole number c=0

Building one-hop transmission neighborhood list: Two neighbor nodes such as S and P which has their neighbor has $N_{(S)}$ and $N_{(P)}$ individually. Their neighbor list information exchange will be shared through a beacon messages. For example, node S notifies its nearest neighbor N(S) with a periodic beacon message.

Building two-hop transmission neighborhood list: Each node will request its neighbors to collect information about their neighbors list by way of transmitting beacon messages to its neighbors. This will enable each node to hold two hop information about their neighbors. For example, information exchanged between nodes A, B and C. Node(A) sends a beacon message to its neighbor Node(B), after this message was sent, the transmission range of Node(A) is increased to 2r. After this increase, node(A) broadcast beacon message containing node(B) information to its neighbor of node(C) during this message, both nodes B and C will not change their transmission range. After node(C) hears this broadcast, it then verifies the authenticity of node(A) from node(B) because both node A and B had earlier exchange their information in the first broadcast. The beacon frame will be transmitted at regular intervals until packet gets to its destination successfully. After each change in radius of transmitting nodes, a test node updates its neighbor node in the next beacon time [4, 5, 6].

If $N_{(C)}$ contains $N_{(B)}$ but not enclosed in $N_{(A)}$ then wormhole detected

If $N_{(C)}$ contains $N_{(B)}$ and meets $N_{(A)}$ then no wormhole is detected.

The schematic of the proposed algorithm for wormhole attack detection and elimination is given in Figure5 [4].

© 2018, IJCSMC All Rights Reserved

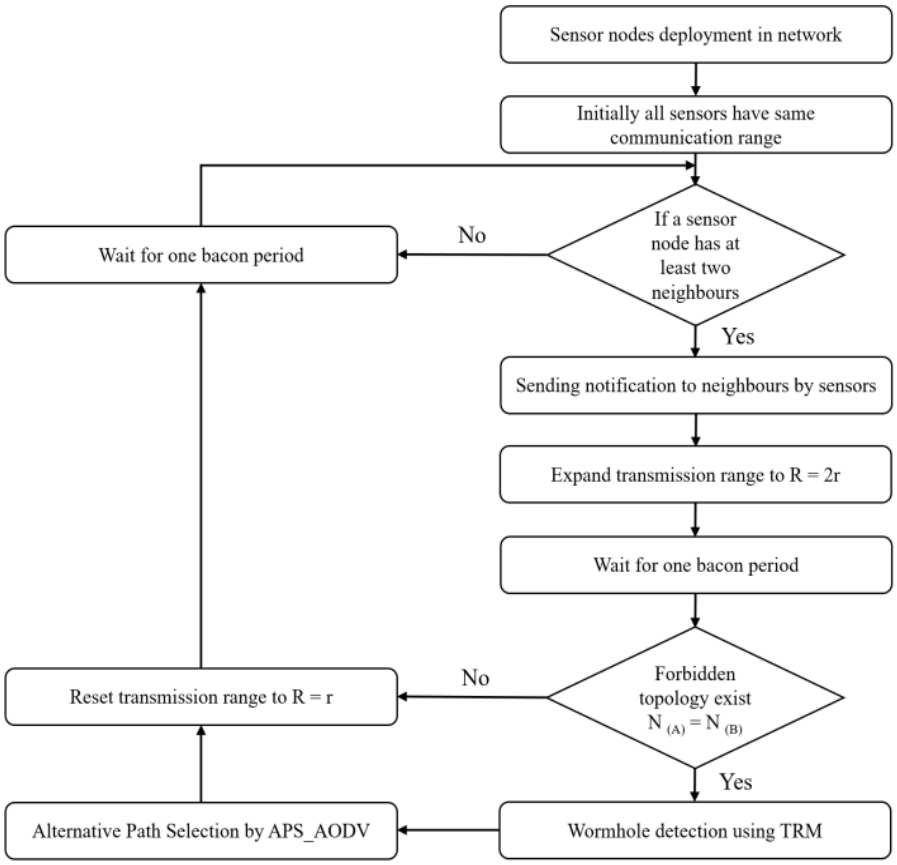

Figure 5: flowchart of proposed algorithm.

F. BLACK-HOLE ATTACK

The black-hole attack is a denial of service attacks which drawdown the system traffic to a specific malicious node. The attack node in this sort of attack act malevolent in the course revelation process, this is finished by sending a phony course answer message to an asking for source hub when it sends a course ask for message with a phony goal succession number to trick the source node that it is the most brief way to the goal [9].

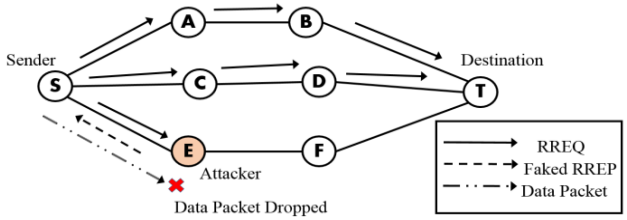

Figure 6: Black-hole Attack.

The system is presently exposed to a directing attack. The attack is done in four situations as pursues:

- **i.** One Black hole attacker.
- **ii.** Ten percent of total nodes as Black hole attackers.
- **iii.** Twenty percent of total nodes as Black hole attackers.
- **iv.** Thirty percent of total nodes as Black hole attackers.

© 2018, IJCSMC All Rights Reserved

G. BLACK-HOLE ATTACK COUNTERMESURES

We present the flow chart of Black-hole (B-H) detection given in Figure 7 [7].

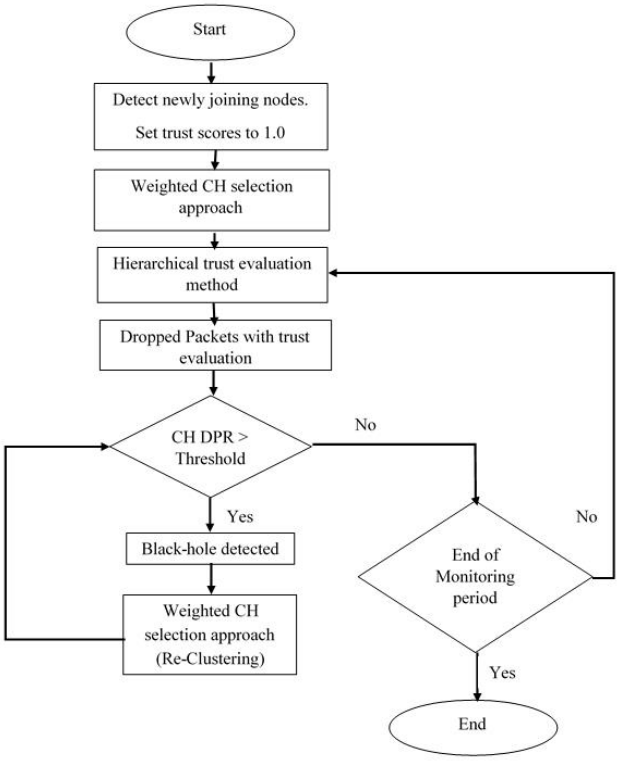

Figure 7: Flow chart of Black-hole (B-H) detection.

The overview of the proposed approach is shown in the following diagram. This strategy is used in MANET but we can use this in black-hole attack on Wireless Sensor Networks as well with little modification [8].

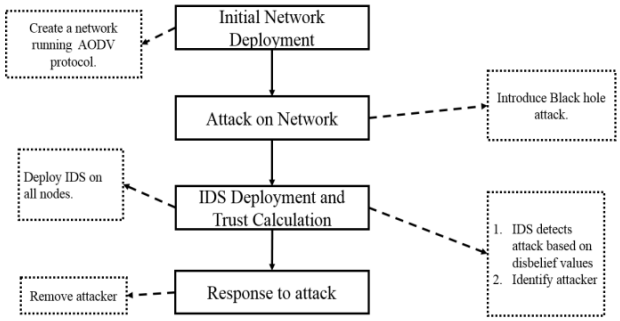

Figure 8: Workflow diagram of planned methodology.

H. GRAY HOLE ATTACK

In Gray Hole attack [14], attack node selectively drops the packet. In the network of nodes if any data packet lost occurs continuously then by traffic analysis it becomes easy to guess the malicious node. Therefore, Grey-hole attackers drop the fraction of message selectively.

There are two conditions for selective forward attacks.

i. Malicious node can drop all User Datagram packet (UDP) packets and forward Transfer Control Protocol (TCP) packets.
ii. Dropping packets by following some probabilistic distribution.

© 2018, IJCSMC All Rights Reserved

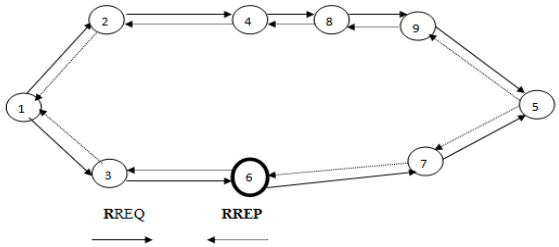

Figure 9: Gray- hole Attack.

I. GRAY -HOLE ATTACK COUNTERMESURES

In this study, the authors proposed an algorithm on AODV protocol. In this algorithm, they tried to understand the behavior of nodes in network, identify destructive nodes and delete them from routing. By increasing the traffic, the destructive nodes increase.

The principles of proposed algorithm are given as follows [14] and [15]:

a. Information about the node's activities including the number of added data, the number of received data and the number of received responses will be saved and analyzed.
b. The request packet has been sent to the neighbor's ideas about the node which sends route reply RREP.
c. Saved information has been received in neighbor's nodes related to sender node RREP.
d. Received information about the destructive node has been considered.
e. A packet of danger alarm for quarantining the destructive node has been sent and it has been developed in all networks.
f. The nodes in quarantine have been deleted from the Routing process.

This algorithm is also capable of identifying the destructive nodes using the following rules:

a. The node which sends a RREP to sender node route request RREQ may be a destructive node.
b. The node which has the least number of hops in RREP and the most number of sequences may be a destructive node.
c. The node which sends the number of packet may be a destructive node.
d. The node which receives a great number of packets and sends only one packet may be a destructive node.
e. The node which receives a few number of packets and does not send them, is absolutely a destructive node.

J. HELLO FLOOD ATTACK

Hello flood attack is a network layer attack. Many routing protocols require nodes to be broadcast Hello packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within normal radio range of the sender. This assumption may sometimes be false; a laptop-class attacker broadcasting routing or other information with large enough communication power could convince every node in the network that the dispute is it neighbors. For example, an opponent advertising a very high quality route to the base station to every node in the network could cause a large number of nodes to effort to use this route, but those nodes sufficiently far away from the adversary would be sending packets into ignorance. Thus the network is left in a state of doubt.

K. HELLO FLOOD ATTACK COUNTERMESURES

Let Pg0(y) is in the control packets generating rate of node y observed by node y0 during time interval T0. Pg1(y) is the packets generating rate of node y observed by node y0 during time interval T1 and Pgz(y) is the control packets generating rate of node y observed by node y0 during time interval Tz. Let Pgi(y) is the control packets generating rate of node y observed by node y0 during time interval Ti. Then the average control packets generating rate is given as

$$P_{gavg}(y) = \sum_{t=1}^{z}(t/z)\ [P_{gt}(y)]$$

now at any interval 'i' if the control packets generating rate of any node is greater than the summation of average control packets generating rate and the control packets generating rate values of the sensor specified in the standard protocol, node is suffering from Hello Flood Attack [20]. Mathematically

$$P_{gi}(y) > P_{gavg}(y) + C$$

where $P_{gi}(y)$ is the control packets generating rate of node y at any given interval i observed by node y_0. C is the control packets generating rate values of the sensor specified in the standard protocol it follows. Node for which

© 2018, IJCSMC All Rights Reserved

equation does not hold true, are malicious and higher control packets generating rate is the identification of hello flood attack.

L. DISTRIBUTED DENIAL OF SERVICE ATTACK

A Distributed Denial of Service (DDoS) attack takes place when many compromised SNs infected by the malicious node act concurrently and are coordinated under the control of a single attacker by flooding the target nodes with bogus requests, exhausting their resources, and forcing them to deny service to the legitimates SNs.

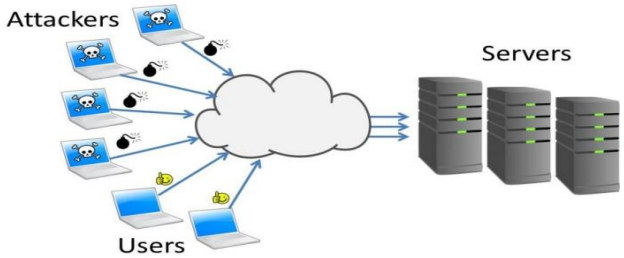

Figure 10: Distributed Denial of service Attack.

Initially, a DoS is a cyber-attack using the Internet with the main aim to make computers' resources unavailable to legitimate users for a period of time. Similarly, DoS attacks may occur any layer of open systems interconnection (OSI) model of WSNs [12]. In this attack, attackers may disrupt the channel by continuously requesting and transmitting over it. It results in starvation for channel access for legitimate SNs.

The attacker aims are given as follows:

- **i.** To deplete the limited energy of legitimate SNs.
- **ii.** To alter or destroy configuration information.
- **iii.** To physically destroy network components.

O. DISTRIBUTED DENIAL OF SERVICE ATTACK COUNTERMESURES

In the present section, defense mechanisms against DDoS attacks have been proposed to detect and remove DDoS attacks [23]. In broader sense, the attacks can be classified into two types, that is, based on deployment location and defense timing. The deployment location can either be Network/Transport Layers or Application Layer. The Network/Transport level DDoS attacks can be divided into source based, destination based, network based or hybrid based. The application-level DDoS attacks are segregated as destination based and hybrid based. Timing-based defense mechanism is categorized into three subtypes. The defense can be implemented before the attack, during the attack or after the attack. In real-time applications, the complete defense mechanism should include all these three types of defenses. Figure 11 shows the classification of defense mechanism against DDoS attacks.

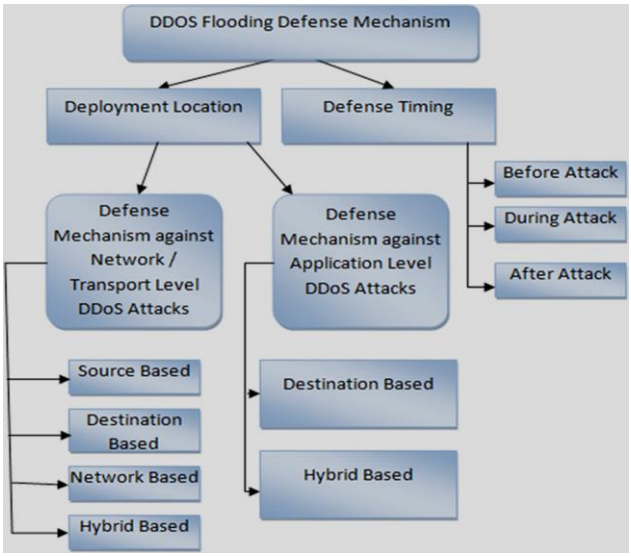

Figure 11: Defense mechanism against DDoS attack.

© 2018, IJCSMC All Rights Reserved

VI. CONCLUSION

Wireless sensor networks are becoming more popular in current times due to their wide range of applications. Sensor communication patterns and their mode of deployment expose them to variety of attacks. This work presents a detail discussion on various types of attacks and trust based approaches to counter these selective attacks on wireless sensor networks. In a future study, we will implement the proposed trust based approaches in a real time event; this will help us to check whether the trust based approaches meet the desired objectives and resources constraint of WSNs.

REFERENCES

[1] R. Singh, J. Singh, and R. Singh, "*A Novel Sybil Attack Detection Technique for Wireless Sensor Networks*", Advances in Computational Sciences and Technology, Vol. 10 No. 2, pp. 185-202, 2017.

[2] R. Singh, J. Singh, and R. Singh, "*TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks*", International Journal of Computer Science and Network Security, Vol.16 No.11, pp. 90-99, 2016.

[3] R. Singh, J. Singh, and R. Singh, "*Sybil Attack countermeasures in Wireless Sensor Networks*", International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.6, No 3, pp. 1-6, 2016.

[4] M. Okunlola Johnson, A. Siddiqui, and A. Karami,, "*A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks*", International Journal of Computer Applications, Vol. 174 - No.4, pp. 1-8, 2017.

[5] R. Kumar Dwivedi, P. Sharma, and R. Kumar, "*Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network*", IEEE-International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 727-732, 2018.

[6] D. Aldhobaiban, K. Elleithy, and L. Almazaydeh, "*Prevention of Wormhole Attacks in Wireless Sensor Networks*", IEEE-conference, pp. 1-5, 2014.

[7] S. Otoum, B. Kantarci, and H. T. Mouftah, "Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring", IEEE-conference, pp. 1-6, 2018.

[8] M. Sen, M. Goldie Meitei, K. Sharma, M. Kanti Ghose, and S. Sinha, "*Mitigating Black Hole Attacks in MANETs Using a Trust-Based Threshold Mechanism*", International Journal of Applied Engineering Research, Vol. 13, No.. 7, pp. 5458-5463, 2018.

[9] M. Abd-El-Azim, H. EL-Din Salah, and M. Ebrahim, "*IDS Against Black-Hole Attack for MANET*", International Journal of Network Security, Vol.20, No.3, pp. 585-592, 2018.

[10] A. Alsumayt, J. Haggerty, and A. Lotfi, "*Using Trust to Detect Denial of Service Attacks in the Internet of Things Over MANETs*", Vol., pp. 1-22, 2017.

[11] S. G. H. Rose, and T. Jayasree, "*A Jamming Detection Technique for WSN Using Timestamp*", IEEE International conference on Intelligent techniques in Control, Optimization and Signal Processing, pp. 1-6, 2017.

[12] R. Bhubaneswar, and R. Ramachandran, "*Prevention of Denial of Service (DoS) Attack in OLSR Protocol Using Fictitious Nodes and ECC Algorithm*", IEEE, pp. 1-5, 2017.

[13] M. Tripathi, M.S.Gaur, and V. Laxmi, "*Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN*", ELSEVIER- International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), pp. 1101-1107, 2013.

[14] S. Shahabi, M. Ghazvini, and M. Bekhtiarian, "*A modified algorithm to improve security and performance of AODV protocol against black hole attack*", Springer-Wireless Network. pp. 1505-1511, 2016.

[15] P. Tiwari, and R. Kumari Kushwaha, "*A Review on Trust Management Approaches in Wireless Sensor Networks*", IJSRSET, Vol. 3 Issue-5, 2017.

[16] A. P. Abidoye, and I. C. Obagbuwa, "*DDoS attacks in WSNs: detection and countermeasures*", IET Wireless Sensor Systems, pp. 52-59, 2017.

[17] A. R. Dhakne, and P. N. Chatur, "*Distributed Trust based Intrusion Detection Approach in Wireless Sensor Network*", IEEE-International Conference Communication, Control and Intelligent Systems (CCIS), pp. 96-101, 2015.

[18] A. R. Dhakne, and P. N. Chatur, "*Design of Hierarchical Trust based Intrusion Detection System for Wireless Sensor Network (HTBID)*", International Journal of Applied Engineering Research, Vol. 12, pp. 1772-1778, 2017.

[19] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao., "*TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks*", Hindawai- International Journal of Distributed Sensor Networks Vol. 2014, Article ID 209436, pp. 1-14, 2014.

© 2018, IJCSMC All Rights Reserved

[20] S. Muhammad Sajjada, S. Hussain Boukb, and M. Yousaf, "*Neighbor Node Trust Based Intrusion Detection System for WSN*", ELSEVIER- Internat ional Conference on Emerging Ubiquitous Systems and Pervasive Networks, pp. 183-188, 2015.

[21] Jeelani, M. Rana, S. Kumar, and A. Zafar, "*Trust Based Approaches of Intrusion Detection Architecture for Wireless Sensor Networks: A Survey*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 10, pp. 107-114, 2018.

[22] M. M. Ozcelik , I. Erdal, and O. Suat, "*A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks*", IEEE-International Symposium on Networks, Computers and Communications, pp. 1-6,2017.

[23] M. Poongodi, and S. Bose, "*A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET*", Springer-Arabian Journal for Science and Engineering, vol. 40, Issue 12, pp. 3583–3594, 2015.

© 2018, IJCSMC All Rights Reserved