Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 2 (2017) pp. 185-202

http://www.ripublication.com

A Novel Sybil Attack Detection Technique for Wireless Sensor Networks

Rupinder Singh[†], Dr. Jatinder Singh[‡] and Dr. Ravinder Singh[‡]

[†]Research Scholar, IKG PTU, Kapurthala, Punjab, India.

[‡]IKG PTU, Kapurthala, Punjab, India.

Abstract

Wireless Sensor Networks (WSNs) are susceptible to Sybil attacks in which malicious node creates a huge number of fake identities in order to gain an excessively high advantage through a Byzantine method. A Sybil node using only one physical device may generate random number of additional node identities and can be used to disrupt normal functioning of the WSN, such as multipath routing which is used to explore multiple disjoint paths between source and destination pairs. Recently, there has been a rising interest in leveraging WSN to mitigate Sybil attacks. Digital certificates are a way used to prove identities; however, they are not feasible in sensor networks. This paper aims to provide, defend against Sybil attack with the help of a trust based technique TBID (Trust Based Identity Detection) in WSN. The proposed scheme is based on the calculating trust values of adjacent sensor nodes. The nodes with the trust values less than a threshold value are detected as malicious (Sybil) node. The feasibility of TBID technique is demonstrated systematically, while experimental results of TBID in exposing Sybil attacks are expansively assessed equally mathematically and numerically. The acquire consequence show that the TBID attains significant attack detection rate than existing techniques.

Keywords: Wireless sensor networks, Malicious, Sybil, Trust based system.

1. INTRODUCTION

Wireless Sensor Network (WSN) is defined as a self-configured and infrastructure-less wireless networks, which is used to monitor the environment or physical conditions, such as temperature, sound, wind direction, humidity, pressure, illumination intensity, speed, chemical concentrations, vibration intensity, power-line voltage, sound intensity, pollutant levels and so on. WSN co-operatively passes the data gathered through the sensors to a central location or sink (also called base station). This data is analyzed for further processing and to take different decisions. Figure 1 shows the structure of a typical WSN. WSN has limited capacity of processing speed, communication bandwidth, and storage. The WSNs due to limitations are inherently resource constrained and are vulnerable to various attacks. The inbuilt complexity of the applied security algorithms also adds to the difficulty of providing security to WSNs.

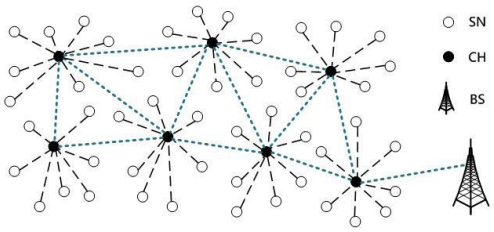

Figure 1: A typical WSN

The proposed security techniques for WSNs in the past assumed that almost all sensor nodes are cooperative and trustworthy, but the same is not true for most of the cases for many sensor network applications today. A large number of attacks are possible in WSN including tampering, jamming, hello flood, exhausting, wormhole, collision, sinkhole, Sybil, flooding, denial-of-service, cloning.

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 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.

In this paper, we first discuss the Sybil attack, trust based system and related works. In the next section of the paper, we describe our Trust Based Identity Detection (TBID) technique for countermeasure against Sybil attack in WSNs. The proposed scheme is based on calculating trust values of adjacent nodes and the nodes with the trust values less than the threshold value are detected as malicious (Sybil) nodes. We implement our proposed technique in ns2, provide the results and discuss possible future work.

2. SYBIL ATTACK AND TRUST BASED SYSTEMS

A variety 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 affecting the routing in the sensor networks. A large number of network security schemes are available for the protection of WSNs from Sybil attack. In this section of the paper, the concept of Sybil attack and trust based system is discussed.

2.1 Sybil Attack

In WSNs, each node is recognized as one entity and just one single abstract idea is presented of an identity. Therefore, in WSNs nodes are susceptible to any scheme that allows identities to be falsified or forged. An attack that results in such a malicious activity is called the Sybil attack. So, a single node in Sybil attack intentionally and illegitimately produces numerous false or forge identities to sensor nodes in the WSN. This is done by either stealing legal identities of other nodes or creating new (fake) identities. A Sybil node in the network is a disobedient nodes extra identity. As a result, a single entity of the network may get a selected number of times (depending on number of identities) in order to contribute in network operations that basically relies on redundancy, thereby in this way it can control the outcome of the operation in order to defeat the redundancy mechanisms. Sybil attack can be activated while broadcasting without the use of any central authority. This central authority of the network may help in the identification of the identities of sensor nodes. Sybil attacker can have different identities; this is done by sending messages with multiple identifiers. Such a malicious sensor node replicates its multiple copies in order to damage the network. One of important observation done about the Sybil attack is that it violates one-to-one mapping between entities and identity in WSN. Figure 2 provides a scenario of Sybil attack.

For detecting a Sybil attack, it is very necessary to recognize the ways in which the network is attacked. The attack can be divided into following three ways:

1) Direct and Indirect Communication

In direct Sybil attack, the legal nodes communicate openly with the Sybil nodes in the network, whereas in indirect attack, this communication is done with the help of malicious nodes.

2) Fabricated and stolen identities

In this type of Sybil attack, a malicious node constructs a new identity for itself. This new identity is based on the identities of the legitimate nodes. The process when these malicious nodes communicate with their next neighboring nodes, they make use of any one of fake identities. This result in confusion in the network and it may collapse the entire network. In stolen identities case, the attacker first identifies legitimate existing identities and stole it. This type of Sybil attack may go unidentified in the network in the case of destroying of the node whose identity has been stolen. Node identity replication is done in the case when the same identities are used for a number of times in the same places in the sensor network

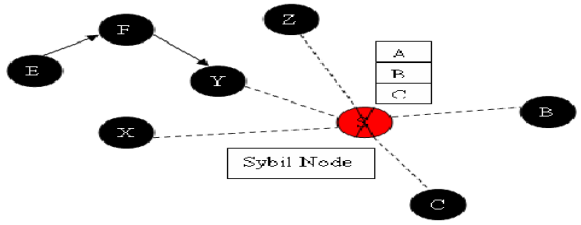

Figure 2: Sybil attack

3) Simultaneous and Non-simultaneous attack
In the simultaneous type of Sybil attack, all the Sybil identities participate simultaneously in the sensor network. Due to one identity appearing at a time, cycling through the identities will make it to appear simultaneously. In 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.

A variety of techniques have been proposed in the literature [1] for tackling with Sybil attack. These include Message authentication, TDOA method, Random password comparison method, Neighborhood RSS based approach, SYBILSECURE technique, Genetic algorithm, Genetic algorithm two-hop messages approach, P2DAP approach, Compare and match approach, Energy and hop based detection, Threshold elgamal key management scheme, Optimized secure routing protocol, RSSI-based scheme, RSSI channel-based detection, UWB ranging-based information and so on. Proposed technique TBID make use of trust based system for the detection of Sybil node which is described in the next part of this section of the paper.

2.2 Trust Based Concept
Wang et al. [2] proposed the concept of trust computation based IDS for Mobile Ad-hoc Networks (MANETs) based on the trust variations along with a chain of evidences. In this trust based systems, the evaluation of the node is approved out regularly. A trust evaluation and reputation inter-changeability based IDS mechanism is presented by Ebinger et al. [3]. In this work, the mixture of trust, reputation, and confidence along with trustworthiness is used as an improvement for the intrusion detection. Various trust management mechanisms are proposed in [4][5][6] for WSNs. The main work of these proposed works comprises security of the systems along with the reliability of information. In [7], a trust based IDS is proposed for cluster based WSNs. In the above proposed work, Cluster head (CH) is used to perform the trust computation and assessment of sensor nodes in the cluster. Honesty, supportiveness, and energy consumptions are the assessment metrics used for detection of malicious activity. The base station is used to evaluate the trust level of CH. In [9][10][11] mean node detection is carried out based on the neighbor node calculation.

Trust is a term that is used for the dependability of an entity. It is a probability of an individual node A that expects individual node B to perform a given task at a particular time. The idea of reputation (that is collecting data concerning the status of a consecutive sensor node) is linked to the trustworthiness. Trust depends upon the ratings of consecutive nodes in the WSN. If the ratings of the consecutive node in the network are over the threshold (accepted value) then the node for further transfer of data will be trusted. Trusting on self detecting misbehaviour of nodes in the network is risky. That is why collaboration between neighboring sensor nodes is required. The data transfer situation is shown in figure 3. Node A via node D manages trust of node D for future transfer of data. When node A forward data to D, node D receives the data and acknowledges this to node A. Node D may or may not transfers data to the subsequently succeeding node in the sensor network. If the node A someway knows that the node D successfully forwarded data, then node A is going to assume that node D is trusted one. After repetitive transfers of data, if the trust value reaches lower than the threshold value, then node A is going to compare trust value of its neighboring node B along with node C that are used for transferring data through the node D. If sensor nodes D is trusted with nodes B and C, then node A is going to set up a new route for data transfer by avoiding node D.

2.3 Related Works

Although some work has been proposed in the literature for the detection of Sybil attack using trust concept in MANET and other systems, but the design of efficient trust based approach for detection of Sybil attack in wireless sensor network is still an open challenge. This motivated as to design a novel technique based on trust concept for detection of Sybil attack in WSN. The Sybil node is detected by observing the number of times it change its identity and the fact whether it will forward the packets or not. Therefore, the different parameters concern with the probability of forwarding successfully data, forwarding incorrect data, data receiving etc. are included in form of equations. The work is unique in the way that till date no work is available in the literature that makes use of trust model for detection of Sybil attack in WSN. Here we discuss some of the related work in the literature.

Aditipaul et al. [13] discusses the impact of Sybil attack in MANET and provides a new approach towards the Sybil attack detection based on trust based model which incorporates the concept of fuzzy expert system and neural network. Fuzzy expert system is used for assigning trust values to the nodes of an ad-hoc network and the learning capability of neural network is used to find out the behavioral discrimination of the Sybil nodes.

Huanhuan Zhang et al. [23] discussed the anonymous nature of online social networks that are vulnerable to the Sybil attack, in which an attacker can fabricate several dummy identities to attack the systems. Authors propose a unified ranking mechanism by leveraging trust and distrust in social networks against such kind of attacks based on a variant of the Page Rank-like model. Authors use existing topological anti-Sybil

algorithms as a subroutine to produce reliable Sybil seeds. To enhance the robustness of these approaches against target attacks, authors also introduce an effective similarity-based graph pruning technique utilizing local structure similarity.

Shivani Kanwar et al. [24] in their paper discuss that trust and security remain a key concern in VANET since a simple mistake can have catastrophic consequence. According to authors, a crucial point in VANET is how to trust the information transmitted when the neighboring vehicles are rapidly changing and moving in and out of range. A trust evaluation based security solution is proposed as countermeasure against Sybil attack to provide effective security decision on data protection, secure routing and other network activities. The authors in order to overcome Sybil attack present trust algorithm for detecting Sybil attacks in VANET. The simulation results according to authors show that algorithm is effective in the detection of malicious nodes in VANET and the probability of malicious to become cluster head is less.

Guojun Wang et al. [19] discussed that passive and active attacks have pushed away potential business firms and individuals whose aim is to get the best benefit in ecommerce with minimal losses and the attacks occur during interactions between the trading peers as a transaction takes place. In this paper, authors propose how to address Sybil attack, an active attack, in which peers can have bogus and multiple identities to fake their owns. According to authors, most existing work, which concentrates on social networks and trusted certification, has not been able to prevent Sybil attack peers from doing transactions. Authors work exploits the neighbor similarity trust relationship to address Sybil attack. In the proposed approach, duplicated Sybil attack peers can be identified as the neighbor peers become acquainted and hence more trusted to each other.

Noor Alsaedi et al. [25] proposed a lightweight trust system using energy as a metric parameter for a hierarchical WSN for dealing with Sybil attack in WSNs. According to authors, the performance evaluation of this system shows efficiency and scalability for detecting Sybil attacks in terms of true and false positive detection in a heterogeneous WSN. In addition, this system reduces the communication overhead in the network by cancelling feedback and recommendations among sensor nodes.

3. TRUST BASED IDENTITY DETECTION (TBID)

This section of the paper discusses network assumptions and the proposed technique TBID.

3.1 Sensor Network Assumption

WSN is composed of small sized sensors that are involved in sending, forwarding, and receiving packets (information). It is assumed that n sensor nodes are distributed within the area of network forming clusters with each having a CH. All the sensor nodes are also assumed to have similar capabilities along with similar workload and their behavior is similar under normal conditions. There exists a malicious node

(Sybil) who do alteration or dropping of data packets before forwarding them. These malicious A have network resource similar to normal nodes, but have different behavior as compared to others. In WSNs the data transforming is divided into various "shares"; the nodes that are involved in forwarding packets (shares) are known as forwarding sensor nodes. Each sensor node continuously listens the network channel in order to observe the behavior of its neighbors (only 1- hop). A sensor node A can hear message to and from neighbor node B that is concerned with the process of packet transmission. It is also assumed that a MAC layer protocol exists in the network that is used to manage broadcasting of neighbors to avoid occurrence of a collision. The modeling of neighbor's behavior is done with α terms of metrics attribute as f(a) = (f_1(a), f_2(a), ..., f_α(a)). Every metric represent the activity of node in one of the feature as shown in figure 5. Examples of such activities are the number of packets being delayed/sent/dropped in one unit time. After the detection of malicious nodes by A, A excludes it during the selection of next-hop forwarding node. This is done in order to assure the security of the network.

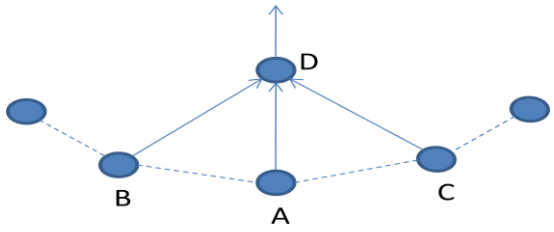

Figure 3: Trust scenario

3.2 Trust Model

A TBID technique for countering Sybil attack in WSN is discussed here. Trust based systems are one of the mechanisms that can be used for tackling with Sybil attack in WSNs. A lightweight neighbor sensor node trust computation based anomaly intrusion detection technique TBID is proposed in this paper. This trust basically depends on the cooperative and trusting nature of sensor nodes in the WSN. The TBID method detects and isolates the malicious (Sybil) node from the sensor network.

In Sybil attack, the malicious nodes can change its identity time to time in order to get undetected and due to this denial of service may occur in the sensor network. Here, a novel technique TBID based on trust values is proposed which is responsible to identify and separate mean sensor nodes from the network. In TBID technique, the sensor network is divided into cluster with each cluster having a CH. Each node in a cluster calculates the trust value of its neighbor and sends it to the CH in the form of a message. The trust value of a node is calculated based on the number of times a node changes its ID. Every time a node changes its ID, it has different neighbors. This will

result in reducing the trust of a node. The CH calculates the average trust value of each node in the cluster from the information received from different nodes. A node is declared as Sybil node if its average trust value is less than the threshold value (i.e. δ). The working of TBID is illustrated in figure 4.

The working of proposed TBID technique detects the nodes to be malicious (Sybil) if their behaviors are observed to be "abnormal" as compared to usual sensors nodes. The proposed scheme divides the working of trust system into the following three phases: Monitoring node behavior, calculating trust values, and filtering Sybil nodes.

1) Building Trust Management

For the selection of faithful forwarding nodes in the sensor network from neighbor nodes, each sensor node needs to decide for a trust management policy that is local. This strategy will focus on constructing a trust, association between neighbor sensor nodes in the network. Data transfer paths from source to destination node are constructed in sensor network as concatenating contacts that follows trust association in trust management. In the trust managing system, the value of trust for every neighbor sensor node depends on evaluation of its various behavior factors shown in figure 5. If the calculated value of trust of a neighbor node is lower than a specified trust threshold δ, then this neighbor node is considered as Sybil node. The relationship between this Sybil node with neighbor nodes is set to be faithlessness.

For every node A in the cluster, by computing trust (T_A) of each neighbor node B, node A select "believable" neighbor node B_B as forwarder node in the list of its neighbor nodes. The node B is able to be eligible as trusted neighbor only if

$T_B \geq \delta$……. (1)

After sending data to forwarders, sensor node A honestly monitors network behavior of forwarders. By the estimate of behavior, the sensor node calculates a fresh trust value. This new value is used for next forwarding and sensor node updates its trust association with this fresh value.

Let $\alpha(u)$, $\beta(u)$, $\lambda(u)$ be set of neighbor "friend" nodes selected as forwarding nodes of the node u. Let α_n, β_n, λ_n be the number of sensor nodes in α, β, and λ respectively. Any node that is un-trusted can be chosen as a forwarding node, therefore

$\lambda \subseteq \beta \subseteq \alpha$ ∀node v ∈ α (u) …….(2)
Has m pieces of behavior information.

The node evaluates the behavior of the data forwarder B_B in x metrics terms. Let $P_B(A_t)$, $P_B(\overline{A_t})$, $P_B(R_t)$ be probability of forwarding successfully data, forwarding incorrect data, and data receiving by node B during the t iteration.

2) Calculating Trust Value

a) Evaluating the degree of Behavior Difference: For making differences among normal and Sybil nodes, we apply trust based technique i.e. TBID. The technique makes use of a feature of Sybil node in which each Sybil node changes its neighbors due to change in its ID. A sensor node "participate" in the route established for data transmission as one process of transmitting and we assume that it has completed iteration. Also, suppose that sensor node B finished t iterations. Then, a characteristic vector for the current and behaviors can be defined as:

$$Y_t^f(B) = (X_1^f(B), X_2^f(B), .., X_{t-1}^f(B), X_t^f(B)) \quad \ldots\ldots\ldots\ldots (3)$$

Where $Y_t^f(B)$ denotes inaccurately forwarding number because of the f^{th} irregular behavior of B node. From this defined vector, we are able to gain the irregular behavior node state and its abnormal behavior of history. The incorrectly forwarding data can be expressed in terms of the weighted sum for each one of the abnormal behavior vector given below:

$$P_B(A_t|R_t) = \sum_{k=1}^{q} W\binom{k}{t}(A_t^k|R_t^k) \quad \ldots\ldots\ldots\ldots\ldots (4)$$

Here, $P_B(A_t|R_t)$ is the incorrectly forwarding data conditional probability that is based on data received for sensor node B during t iteration. The successfully forwarding conditional probability based on receiving data for the sensor node B at iteration t can be defined as:

$$P_B(\overline{A_t}|R_t) = 1 - P_B(|R_t) \quad \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

b) Evaluation of Trust Value: A sensor nodes data forwarding behavior and information from its past experience for node B at t^{th} iteration is used to obtain the following three priori probabilities: the successfully data forwarding probability $P_B(A_t)$, the incorrectly forwarding data probability $P_B(\overline{A_t})$, and the data receiving probability of $P_B(R_t)$. The computation of these probabilities is as follows:

$$P_B(\overline{A_t}) = 1 - P_B(A_t) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

$$P_B(A_t) = (g_B(x_t)/h_B(\theta_t)) \quad \ldots\ldots\ldots\ldots\ldots\ldots (7)$$

$$P_B(R_t) = (h_B(\theta_t)/\sum_{l\in\lambda(u)} h_l(\theta_t)) \quad \ldots\ldots\ldots\ldots (8)$$

Here, $h_B(\theta_t)$ is defined as the total number of receiving data packets and $g_B(x_t)$ is the incorrectly forwarded total number of data packets at iteration t. $\sum_{l\in\lambda(u)} h_l(\theta_t)$ Is the total number of packets that are received by sensor node B and neighbor sensor nodes $\lambda(u)$.

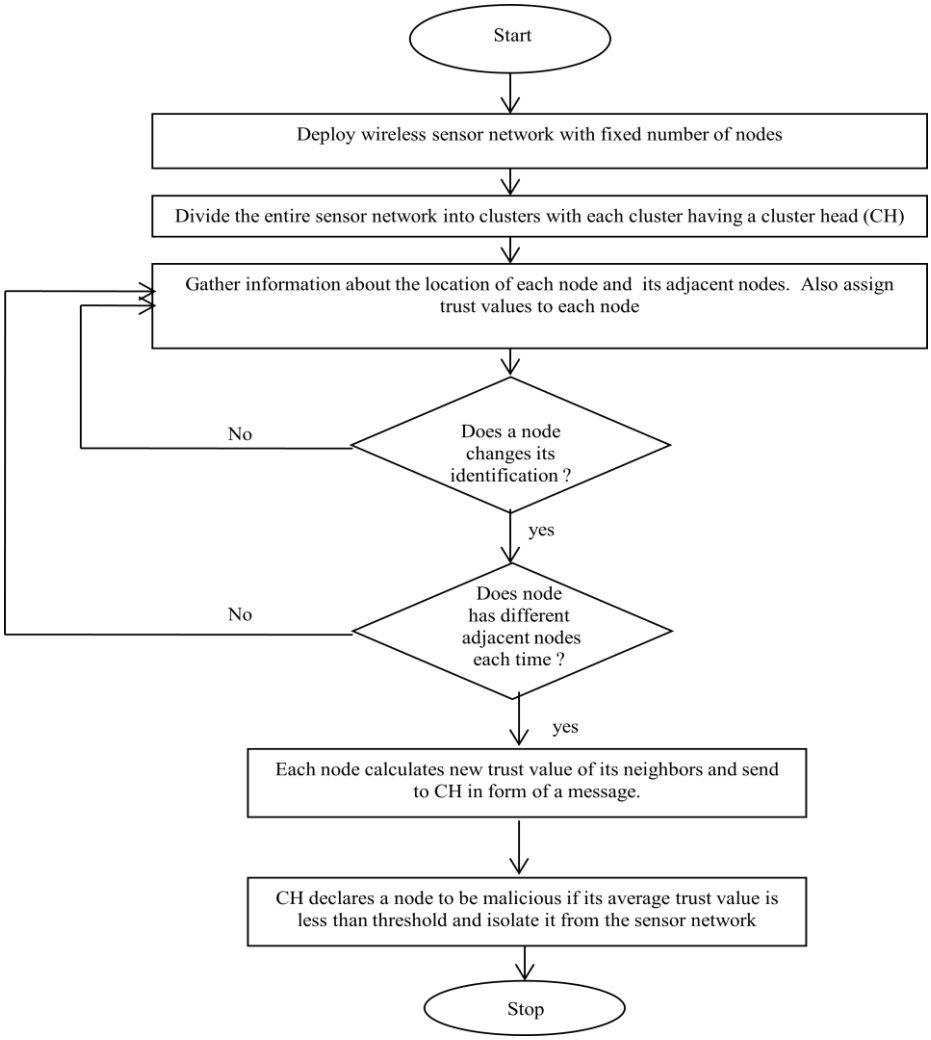

Figure 4: Flowchart of TBID

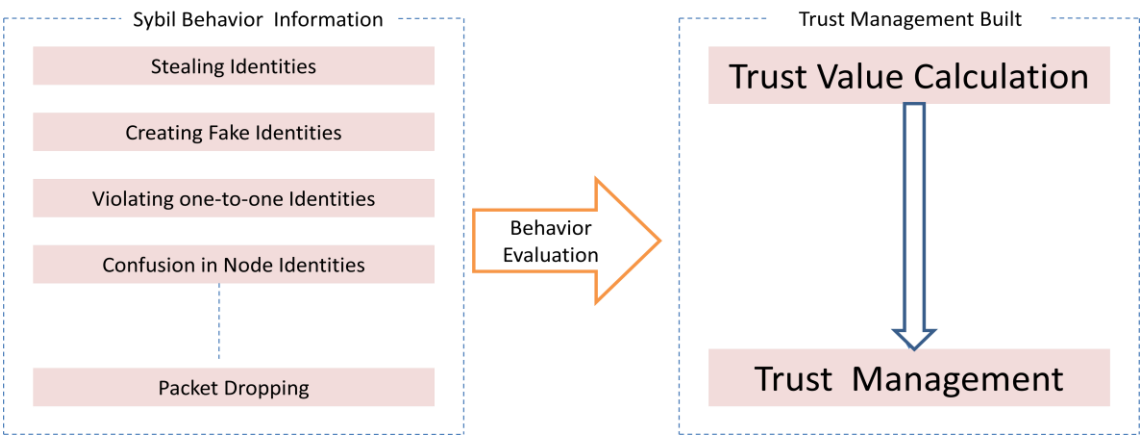

Figure 5: Building of Sybil trust management

The trust of sensor node is defined as the probability that node B is selected. This is done according to the probability that node B successfully forward the data at the node is not a Sybil node and does not change its identity:

$T_t(v) = P_B(R_t \mid \overline{A_t})$ …….(9)

The above equation can be expanded for the calculation of the trust value of a sensor node as follows:

$T_t(v) = P_B(R_t \mid \overline{A_t}) = (P_B(R_t)P_B(\overline{A_t} \mid R_t))/(P_B(\overline{A_t}))$ …….(10)

c) Separating Sybil Nodes: Consider direct calculations by sensor node so as to assess neighbor nodes trust, this may result in subjectivity. In order to judge additional comprehensively, before selecting, decision maker that is CH will broadcast every one of its neighbors that the route selecting process is starting. On receiving of broadcasting message, every neighbor sensor node in α(u) is to create L(u) that is a list of its neighbor node sand send this list to decision make CH. The list of values calculated is set in the form of a message shown in Figure 6, this message includes a list of all the neighbors along with trust values. From these sensor nodes, some neighbor nodes do not contribute in the process of data transmitting. The trust value of these neighbors is unaltered. In sensor network the range of communication is restricted for each sensor node therefore a node B is not able to monitor each node in α(u). The broadcasting message of node B contains a portion of decision CH range sensor nodes. The CH combines received messages for every sensor node in the network.

In order to make the concept clear, a combined broadcasting message received is provided in Figure 7. The matrix of trust value for sensor node in a particular cluster with CH contains the assessed trust value of each sensor node calculated by another neighbor node. If the sensor node i does not overhead on the sensor node j, then the $Value_{i,j}$ is -1. It is also considered that a sensor node cannot watch itself, therefore -1 is set as $Value_{i,i.}$

CH_{ID}	Number	ID_1	$Value_1$	.....	ID_{n-1}	$Value_{n-1}$

Here,
CH_{ID}: Cluster head ID
Number: The no. of nodes in L(v)
ID_i: Node B_i ID
$Value_i$: The trust value of node B_i

Figure 6: Node B trust value list message format.

	ID_1	ID_2	.....	ID_{n-1}	ID_n
ID_1	-1	$Value_{1,2}$	.....	$Value_{1,n-1}$	$Value_{1,n}$
ID_2	$Value_{2,1}$	-1	.....	$Value_{2,n-1}$	$Value_{2,n}$
.....	.....	.....	-1	.....	.....
ID_{n-1}	$Value_{n-1,1}$	$Value_{n-1,2}$	.....	-1	$Value_{n-1,n}$
ID_n	$Value_{n,1}$	$Value_{n,2}$	.....	$Value_{n,n-1}$	-1

ID_i: the ID of node i in α(u)
$Value_{i,j}$: node i trust value computed by j

Figure 7:α(u) nodes trust value matrix.

The Sybil nodes may broadcast the message to CH similar with normal sensor nodes making the exposure process more complicated. Therefore, it is required that suspected Sybil nodes should be filtered first. For a neighbor sensor node in the cluster, sensor node u calculates the common value of the trust as:

$$Average_j = ((Value_{1,j} + Value_{2,j} + ... + Value_{n,j})/n_j) \quad \text{.....(11)}$$

Here, n_j is no. of its watch nodes in the cluster. The calculated values, sensor nodes have to be in [0, 1] range. In TBID scheme, if $Average_i < \delta$, then the sensor node iis a Sybil node. In the provided matrix of trust values, all the trust values will be set as -1from these Sybil nodes. Finally, all the Sybil nodes are isolated from the sensor network. After isolation of Sybil nodes in the sensor network, the sensor node u calculates average trust value, making use of equation (11). This trust value (average) is used as the final value of trust for secure routing in the sensor network.

4. SIMULATION-BASED IMPLEMENTATION AND EXPERIMENTAL RESULTS

The performance of TBID was thoroughly tested in a simulation environment for wireless sensor network developed in NS-2, with the simulation parameters used being defined in Table 1.

The first step in the simulation is to deploy WSN by defining the network source node and destination nodes. We first create a sensor network with 42 nodes and then trigger a Sybil attack as shown in figure 8. The sensor network is divided into different clusters. Each cluster has its own CH and is represented with a different color as shown in the figure 8. The adjacent nodes of the destination node will respond back to the source node with the route reply packets. The source node selects the best path from source to destination on the basis of the sequence number and hop count. It is

assumed in the simulation that a single Sybil node existed in the sensor network with all nodes having identical IEEE 802.11b hardware. These sensor nodes with the exception of the Sybil node are randomly distributed within the network area. Node 35 is the malicious (Sybil) node in the network and after the implementation of TBID technique this malicious node is isolated from the sensor network. In the next part of this section of paper, we provide various graphs to show the effectiveness of the proposed technique.

The algorithm for the TBID works as the source waits for the destination to send an acknowledgement to it after every 10th packet. If source receives the acknowledgement from destination, then there is no misbehavior in the WSN and the process continues as normal. But if the destination fails to acknowledge the data packets for a time period, then detection methodology starts its functionality. The established path will be tested to detect and isolate the presence of malicious nodes (if any) from the WSN. Here, we apply the proposed approach of TBID technique to locate any possible Sybil during the route discovery process. If a malicious node is detected by neighbor node, the information is sent to CH in the form of message format of figure 6. The CH makes use of trust value matrix to locate and isolate the Sybil nodes in the sensor networks.

Table 1: Simulation parameters

Parameter	**Value**
Simulator used	NS 2.35
Area (meter)	1600X900
No. of nodes	42
Routing protocol	DSDV
Channel type	Wireless
Packet size	512 byte
Mobility model	Two ray ground
	Propagation model

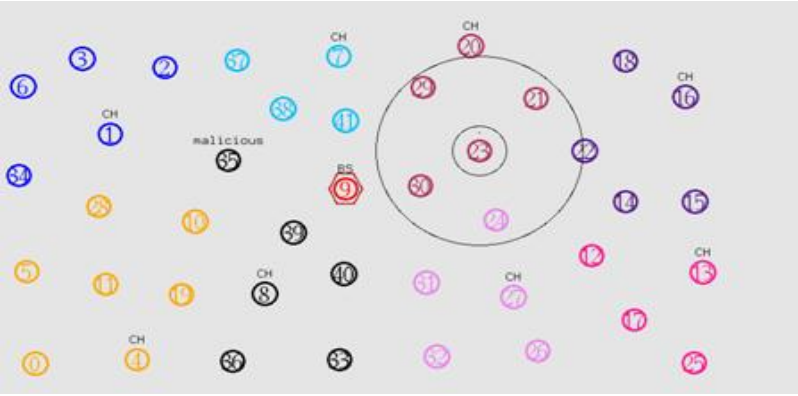

Figure 8: Sybil attack scenarioin WSN

4.1 Throughput of TBID

In the first experiment, we measure the sensor network throughput as this is one of the crucial network parameter. Network throughput refers to the average rate of successful delivered packets. Throughput is calculated depending on total number of packets that are received at the destination in sensor network per unit of time. Throughput is defined as

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

Figure 9 shows the throughput analysis in the case of the sensor network without a Sybil attack (DSDV), under Sybil attack, and after implementation of TBID. The figure clearly shows that the proposed technique after the isolation of the Sybil results in the increase of throughput.

4.2 Packet Delivery Ratio Of TBID

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

PDR = (Packets received/packets generated) * 100

Figure 10 shows the PDR analysis in the case of the sensor network without a Sybil attack (DSDV), under Sybil attack, and after implementation of TBID. The figure clearly shows that the proposed technique 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.

4.3 Delay of TBID

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

Delay = $\sum$ (arrive time – send time) / $\sum$ Number of connections

The lesser value of end to end delay is an indicator of the better performance of the protocol. Figure 11 shows the end-to-end delay in the case of sensor network under Sybil attack, without Sybil (DSDV), and after the implementation of TBID. The figure shows that the proposed technique results in the decrease in end-to-end delay

4.4 Overhead of TBID

Overhead is the excess time taken by the protocol to deliver the packets at the destination. Sybil attack 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 12 shows overhead in the case of sensor network under Sybil attack, without Sybil (DSDV), and after the implementation of TBID. TBID results in decreasing the overhead of the network as shown in the figure 12.

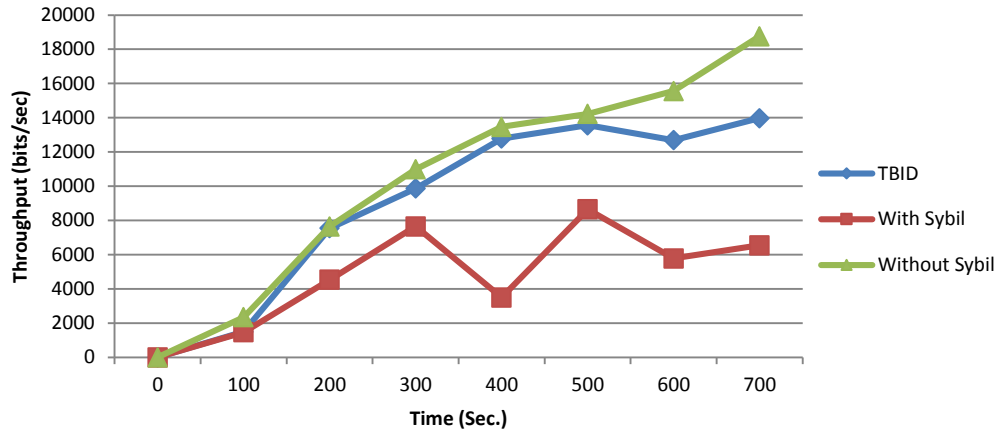

Figure 9: Throughput of TBID

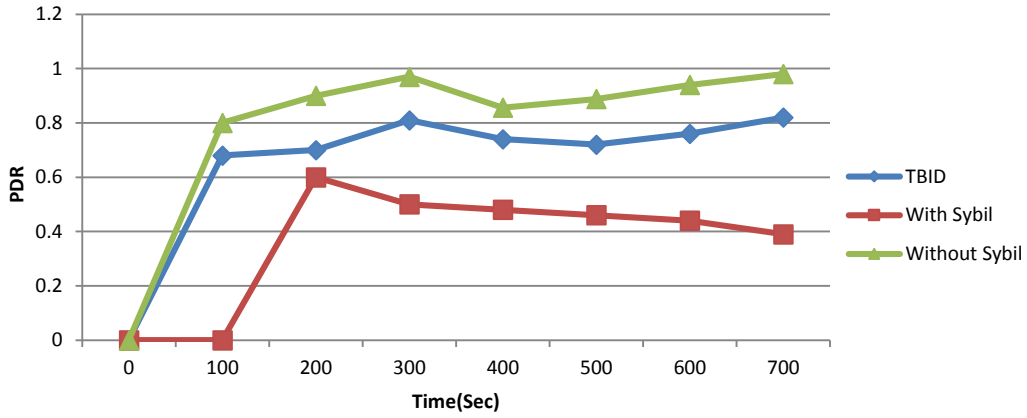

Figure 10: PDR of TBID

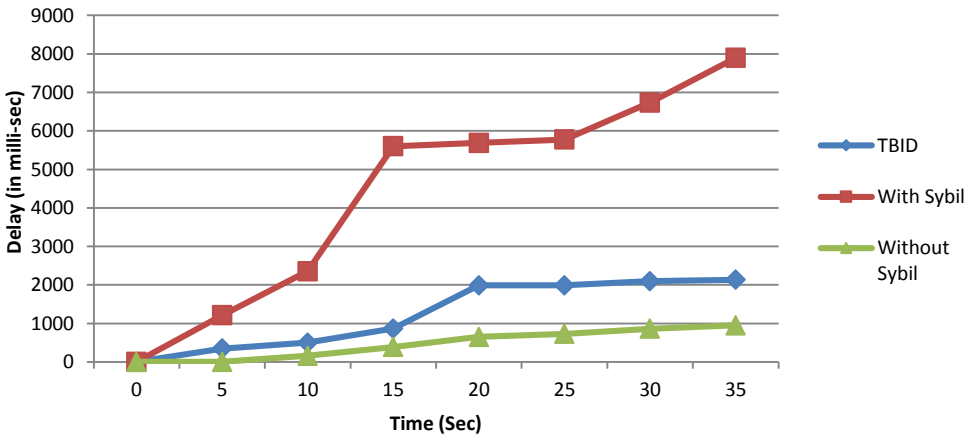

Figure 11: Delay of TBID

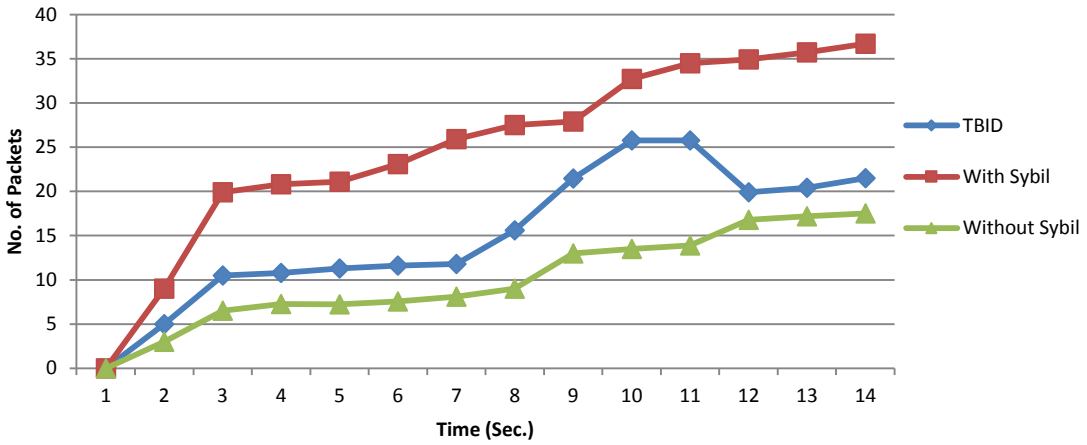

Figure 12: Overhead of TBID

5. CONCLUSION

Sybil attacks in WSNs are severe attacks, addressing Sybil attacks is a crucial issue for the security of WSNs. In this paper, TBID, a trust based scheme for detection of Sybil attack in WSNs is proposed. The sensor network is divided into the clusters with each having a CH. The TBID first assign trust values to each node after gathering information about the position and neighboring nodes of each node. The node that changes identification has unlike neighboring nodes every time, this information will decrease the trust value of the node. Each node in the cluster calculates trust value of neighbor nodes and sends it to the CH in the form of a massage for further processing. The nodes that have average trust value less than a predefined threshold are detected as the malicious (Sybil) nodes and are isolated from the sensor network. The effectiveness of TBID is tested using ns2 and the results show a high performance for the factor of throughput, PDR, delay, overhead. The limitations of the study are that the implementation is done in ns2 with 42 nodes only. We also implemented limited parameters for the working of proposed work. In future, the work will be extended to other routing protocols. The number of nodes will be varied and the more performance parameters will be included for the proposed work.

ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Singh R, Singh J, and Singh R. Sybil Attack Countermeasures in Wireless Sensor Networks. International Journal of Computer Networks and Wireless Communications, Vol. 6, No. 3, May2016.

[2] Wang F, Chen H, Zhao J, and Rong C. IDMTM: A Novel Intrusion Detection Mechanism Based on Trust Model for Ad Hoc Networks. Advanced Information Networking and Applications, 2008.

[3] Ebinger P and Bissmeyer N. TEREC: Trust Evaluation and Reputation Exchange for Cooperative Intrusion Detection in MANETs. Communication Networks and Services Research Conference, 2009.

[4] Ganeriwal S, Balzano L, and Srivastava M. Reputation-based frame work for high integrity sensor networks.ACM Transitions on Sensor Network, vol. 4, no. 3, May 2008.

[5] Liu K, Abu-Ghazaleh N, and Kang K. Location verification and trust management for resilient geographic routing. Journal of Parallel and Distributed Computing, Vol. 67, No. 2, pp. 215-28, 2007.

[6] Shaikh R, Jameel H, Auriol B, Lee H, Lee S, and Song Y. Group-based trust management scheme for clustered wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, Vol. 20, No. 11, PP. 1698-1712, Nov. 2009.

[7] Bao F, Ray I, Chang M, and Cho JH. Trust-Based Intrusion Detection in Wireless Sensor Networks. IEEE International Conference on Communications, 2011.

[8] Stetsko, Folkman L, and Matyayas V. Neighbor-Based Intrusion Detection for Wireless Sensor Networks. International Conference on Wireless and Mobile Communications Los Alamitos, CA, USA, pp. 420-425, 2010.

[9] Liu F, Cheng X, and Chen D. Insider attacker detection in wireless sensor networks. In Proceedings of IEEE INFOCOM, pp. 1937-1945,2007.

[10] Li G, He J, and Fu Y. A group-based intrusion detection scheme in wireless sensor networks. In Proceedings of GPS - Workshops, pp.286-291, IEEE, 2008.

[11] Wu R, Deng X, Lu R, and Shen X. Trust-based anomaly detection in wireless sensor networks. IEEE International Conference on Communications in China (ICCC), 2012.

[12] Zheng Sand Baras J. Trust-assisted anomaly detection and localization in wireless sensor networks. In Proc. IEEE Conf. on Sensor, Mesh and Ad Hoc Comm. and Network (SECON), pp. 386394, 2011.

[13] Paul A, Sinha S, and Pal S. An Efficient Method to Detect Sybil Attack using Trust based Model. Proc. of Int. Conf. on Advances in Computer Science, AETACS, Elsevier, 2013.

[14] Rafeh Rand Khodadai M. Detecting Sybil Nodes in Wireless Sensor Networks using Two-hop Messages. Indian Journal of Science and Technology, Vol. 7(9), 1359–1368, September 2014.

[15] Wang W, Pu D, and Wyglinski A. Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding. IEEEIIFIP International Conference on

Dependable Systems & Networks (DSN), 2010.
[16] Zhou T, Choudhury R, Ning P, and Chakrabarty K. P^2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks. IEEE Journal On Selected Areas in Communications, Vol. 29, No. 3, March 2011.
[17] Fong P. Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. IEEE Symposium on Security and Privacy, 2011.
[18] Abbas S, Merabti M, Llewellyn-Jones D, and Kifayat K. Lightweight Sybil Attack Detection in MANETs. IEEE Systems Journal, Vol. 7, No. 2, June 2013.
[19] Wang G, Musau F, Guo S, and Abdullahi M B. Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce. IEEE Transactions o Parallel and Distributed Systems, December 2013.
[20] Gong NZ, Frank M, and Mittal P. Sybil Belief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection. IEEE Transactions on Information Forensics and Security, Vol. 9, No. 6, June 2014.
[21] Cai L and Rojas-Cessa R. Containing Sybil Attacks on Trust Management Schemes for Peer-to-Peer Networks. IEEE ICC Communication and Information Systems Security Symposium, 2014.
[22] Singh J, Gupta S, and Kaur L. A Cross-Layer Based Intrusion Detection Technique for Wireless Networks. The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.
[23] Zhang H, Xu C, and Zhang J. Exploiting Trust and Distrust Information to Combat Sybil Attack in Online Social Networks. 8th IFIP WG 11.11 International Conference, IFIPTM 2014
Singapore, July 7-10, 2014.
[24] Kanwar S, Joshi S, and Sood M. Detection of Sybil Attack in VANETs by Trust Establishment in Clusters. International Journal of Computer Engineering and Applications, Volume 7, Issue 1, July 2014.
[25] Alsaedi N, Hashim F, and Sali A. Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks. IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia, Nov 2015.