BTEM: Belief based trust evaluvation mechanism for wireless sensor networks

Raja Waseem Anwar, Anazida Zainal, Fatma Outay, Ansar Yasar, Saleem Iqbal

PII: S0167-739X(18)33104-2
DOI: https://doi.org/10.1016/j.future.2019.02.004
Reference: FUTURE 4757

To appear in: *Future Generation Computer Systems*

Received date : 13 December 2018
Revised date : 31 January 2019
Accepted date : 3 February 2019

BTEM: BELIEF BASED TRUST EVALUVATION MECHANISM FOR WIRELESS SENSOR NETWORKS

Raja Waseem Anwar[a], Anazida Zainal[a] , Fatma Outay[b] , Ansar Yasar[c] and Saleem Iqbal[d]

[a]*Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310 Johor Bahru, Malaysia*
[b]*College of Technological Innovation (CIT)- Zayed University, Dubai*
[c]*UHasselt,- Hasselt University, Transportation Research Institute (IMOB)-, Agoralaan, 3590 Diepenbeek, Belgium*
[d]*University Institute of Information Technology, PMAS University, Rawalpindi, Pakistan*

ABSTRACT

With the emergence of WSNs in the recent times, providing trustworthy and reliable data delivery is challenging task due to unique characteristics and constraints of nodes. Malicious node can easily disrupt the integrity of network through the inclusion of false and malicious data and initiate internal attacks. Detection of malicious nodes using trust-based security is an effective and lightweight countermeasure as compared to key based security schemes which incurs higher overhead costs. The WSNs will play greater role in the next-generation IoT systems and a compromised node can jeopardize the availability and authenticity of sensory layer. In this paper, an efficient Belief based trust evaluation mechanism (BTEM) is proposed which isolates the malicious node from trust-worthy nodes and defend against Bad-mouth, On-Off and Denial of Service (DoS) attacks. Bayesian estimation approach is used in gathering direct and In-direct trust values of the sensor nodes which further considers the correlation of the data collected over the time and then estimate imprecise knowledge in decision making for secure delivery of data thus avoiding the malicious nodes. Compared with existing approaches, the proposed BTEM performs better in the detection of malicious node (MN), with lesser delay and improved network throughput.

Keywords: Wireless Sensor Networks, Malicious nodes, Trust, Security, Bayesian estimation;

1 INTRODUCTION

Network reliability and the integrity of collected information are based on trustworthy communication between the deployed sensor nodes. To enhance the cooperation and establishing secure communication in WSN it is important to detect and isolate malicious sensor node which disrupts network communication and drop, the data packets legitimately. Internal network attacks such as malicious node attacks remain a formidable challenge for researchers although various trust and traditional security solutions for WSNs are in place but still there is need to fill this gap. In the recent past wireless sensor networks gained significant popularity due to their wide spread use in variety of applications such as cyber-physical systems, Internet of Things (IoT), disaster response applications such as forest fire monitoring, battle field, environmental and pollution monitoring, health and energy sectors [1-3].

[1]Corresponding Author

E-mail addresses: rajawaseem@gmail.com ([1]Raja Waseem Anwar); anazida@utm.my (Anazida Zainal); fatma.outay@zu.ac.ae (Fatma Outay); ansar.yasar@uhasselt.be (Ansar Yasar); saleem@uaar.edu.pk (Saleem Iqbal).

However, the random and un-attended deployment of these networks where human interaction is difficult sensor networks are prone to failure and suffer from malicious node attack, physical capture and various other types of attacks which are difficult to predict and the integrity of received information is questionable [4, 5]. Securing the network from internal attacks due to malicious node is an important challenge in the deployment of WSNs. Applying the existing and already deployed infrastructure-based network security solutions such as cryptography, authentication and hash functions are able to provide security up to certain extent but finding the malicious node is challenging task due to complexity involved in computation, higher energy consumption and larger memory requirements. Therefore, these existing security solutions cannot prevent the internal attacks effectively. For example, sensor nodes which are deployed at battle field or forest fire detection are extremely security-critical and the breach of network may lead to severe threats and consequences. Trust-based security mechanisms are regarded as an improvement to traditional cryptographic security approaches due to reliability and effectiveness in detection of malicious node and internal attacks [6-8].

Performance degradation due to the inclusion of malicious node into WSN is the real threat. In addition, the malicious nodes are the source of internal attacks. Detecting the malicious node can enhance the performance significantly and increases the network life time. Using trust as a security mechanism in WSNs is new and promising approach as compare to traditional resource constraint cryptographic-based security measures. The context of trust in wireless sensor networks could be described as the degree of confidence level and belief of nodes on each other which is maintained through past interactions, behavior observations and the number of interactions performed directly and indirectly and such actions can be recorded in order to maintain the information which could use later in decision making process [9, 10]. Moreover, trust and reputation-based security mechanisms are more resilient against internal attacks. The inclusion of malicious nodes in the network can limit the communication among the nodes. Consequently, which impacts on network performance. Therefore, it is important to maintain a secure and trust-worthy communication environment through the identification and exclusion of malicious nodes. Hence, successful and reliable node cooperation is assured only when all nodes operate in a trustworthy manner [11]. For such reasons, trust-based security mechanisms pave an improvement and addition to traditional security measures. Forming and estimation of trust among the sensor nodes reduce the risk of internal attacks which allows detection of untrustworthy nodes causing misbehavior and interruption of the normal network operation.

Also, enormous efforts of research has been done in modelling and managing the trust, but these studies mostly consider the aspect of communication interaction among nodes and ignores the data consistency, energy level and periodic re-evaluation of participating nodes since node behavior is constantly changing with respect to context and deployment. In addition, malicious nodes intentionally changing their behavior through fewer number of packets drop (bad behavior) as compared to packet forward ratio (good behavior), such change of behavior is difficult to detect while at the same time network integrity is at threat [11, 12].

In this paper, malicious nodes are identified and isolated using Bayesian estimation approach. Belief based trust evaluation mechanism (BTEM) enhances cooperation and builds trust among the sensor nodes through detection and isolation of malicious nodes. In addition, the proposed mechanism resists against various internal attacks such as On-Off, Bad-mouth and Denial of Service (DoS). Simulation results reveals the improved network performance in terms of malicious node detection rate, increase in trustworthiness level with less false-positive and detection of attacks. The proposed Belief based trust evaluation mechanism (BTEM), is suitable for resource constraint WSNs, due to its design and trust prediction capabilities.

In brief, the main contribution of this paper are as follows;

- The use of Bayesian belief based malicious node detection and isolation mechanism for WSNs.
- Evaluation and validation of the effectiveness of the proposed mechanism.

The rest of the paper is organized as follows: Section 2 highlights the most related trust evaluation mechanisms and schemes that have been presented in the recent past. The proposed BTEM mechanism is presented in Section 3. Simulation details and results of the proposed mechanism are presented in Section 4, followed by concluding remarks and recommendations for future work in Section 5.

2 LITERATURE REVIEW

Identification of malicious nodes is challenge in WSNs, which has attracted academic and industry attention. Some of the studies related to malicious and compromised node detection using trust-based security are briefly reviewed in this section.

To defend against internal attacks, trust and reputation based security mechanisms are in place which evaluates the reliability of the communicating node and identify the malicious node according to the evaluation results [13]. In the emerging world of sensing technologies where the nodes are deployed in an open environment, the network security, protection from adversaries and providing integrity, confidentiality and authentication is highly desirable with better throughput and minimum delay which is difficult to achieve through cryptographic security implementation due to resource constraint nature of sensor nodes. Besides, these traditional security methods are able to defend against external attacks but unable to identifies the internal attacks effectively due to the inclusion of malicious node into network [14]. Therefore, the use of trust-based security has proven to be more resilient against the detection of malicious nodes and towards in achieving reliable data delivery.

Due to various kind of risks, threats and vulnerabilities to WSN, where adversaries are capable of compromising senor node get the key and disrupt the communication. The use of trust as security measure solves the issue of access control, detection of malicious nodes and provides secure end to end trustworthy routing path towards destination. Similarly, the unexpected behaviour, faulty and malicious nodes in the network can be identified through trust evaluation mechanisms. Trust-based security solutions are built on node level through wireless radio transactions with neighboring nodes. The authors in [15], proposed a lightweight distributed trust framework which is resistant to Sybil attacks and protects the user's anonymity. The trust mechanism uses Bayesian and weightage average method for direct and indirect trust calculation Moreover, reputation mechanism is used to disseminate the opinion based decision making.

Group based trust management scheme (GTMS) is proposed by Shaikh et al., [16], which deals with clustered based WSNs. The proposed scheme consists of three levels of trust computation: at the node level, at the Cluster Head (CH) level and at Base Station (BS) level. Total trust is calculated through incorporation of direct and indirect interaction of nodes. Direct calculation of trust is based on successful and unsuccessful transfer of data between nodes while indirect trust incorporates the recommendation of peer nodes. The final trust level is quantified as, trusted and uncertain. The accumulative trust for the particular cluster level is calculated at base station level.

The authors in [17], proposed a Parametrized and Localized Trust Management (PLUS) model where nodes used recommendation and personal for the establishment of trust. The personal reference value is calculated through the count of successful transfer of data packets while recommendation trust is obtained from neighboring nodes. The scheme incorporates integrity check through number of sent packets and uses the reward and penalty mechanism to decide about the node status whether the node is trustworthy or suspected. However, the major issue with the proposed scheme is the assignment of unfair plenty to legitimate nodes which turns into malicious node.

Ganeriwal et al.,[18], design the first trust and reputation based trust model based on Bayesian network. The model monitors the node behavior using a watchdog mechanism. Moreover, the proposed model incorporates beta distribution function for calculating the node reputation using direct and indirect trust which evaluates node trustworthiness level. Besides, the proposed scheme is simple in its implementation, but it does not attack resistant and ignores the malicious nodes detection which is the major limitation of the proposed model. Similarly, the authors in [19] propose a Node Behavioral Strategies Bending belief theory of the trust (NBBTE), which is formulated on the basis of behavior strategy banding D-S belief theory. The proposed mechanism uses various factors for the trust establishment between nodes. First the trust values are obtained using security degree of the network and co-relation of time context which is then combined with fuzzy set theory to measures the achieved trust. Secondly, the difference of obtained evidence is calculated between direct and indirect trust which is then linked with revised D-S evidence combination rule to get the integrated trust value of the nodes.

An attack resistant and lightweight trust management scheme (ReTrust) is proposed in [20], for medical wireless sensor networks which is based on hierarchical network architecture. The proposed scheme calculates the node trust level using sliding time windows and aging factor to identify the malicious behavior of participating nodes. Moreover, the scheme is able to combat the On-off and bad-mouthing attack which improves the network performance and protected the network from malicious nodes. The authors in [21], propose a multidimensional attack resistant trust model (ARTMM) for under water wireless sensor network which computes node trust level using, link trust, node trust and data trust. Moreover, the model incorporates the mobility factor and unreliability of communication channel into account while calculating the direct and in direct trust. Fuzzy logic is used to describe the relationship of trust and attacks which occurs at network, datalink and physical layer.

The authors in [22], proposed an efficient distributed trust model (EDTM). The proposed model uses direct trust and in-direct trust in the form of recommendations from nodes to calculate the total trust. The direct trust of the node is obtained through communication, data and energy trust while indirect trust is calculated based on the recommendation from other nodes. In addition, recommended trust accuracy is improved through trust reliability and familiarity which helps further in the detection of malicious nodes. Similarly, in another work the authors propose a Trust based cross-layer framework (TruFix) [23], which provides defense against various network attacks. Moreover, direct and indirect trust calculation of nodes is considered in the framework, while fuzzy-logic is used for trust estimation and decision making including interlayer exchange of information among the nodes. More recently, Cloud theory based trust evidence generation model (TMC) is proposed in [24], for underwater acoustic sensor network based on game theory. The proposed model calculates the direct trust based on interaction among nodes and indirect trust is acquired in the form of recommendation. Moreover, the model is resilient against various kind of internal attacks such as, Jamming and DoS, bad-mouth and On-off attacks but lack in providing reliability of message delivery among the nodes.

In addition the authors in [25], proposed Trust-based neighbor selection using activation function (AF-TNS) for wireless sensor networks that employs only direct trust and additive metric to evaluate trustworthiness and retainment of trusted neighboring nodes. Also, the proposed scheme isolates the malicious node by considering only direct trust from the neighboring nodes, it exhibits several flaws and vulnerabilities. AF-TNS, incorporates only received data packets for trust calculation which is not an appropriate because the trust level of the sensor nodes varied with time and trusted node become a malicious node due to its energy depletion. Moreover, AF-TNS, didn't consider indirect trust and recommendations which lacks in providing a mechanism to prevent against false information, propagated through malicious node against a trustworthy node. In addition, inclusion of only direct-trust results in higher false-positive rate due to Bad mouth attack and these factors contribute to inaccurate trust estimation and detection of malicious node thereby results in wrong decision making.

A different trust based model known as a novel trust model of dynamic optimization using entropy (Trust-Doe) was proposed [26]. The proposed trust model is able to defend against collusion attack by employing global trust (GT) and divide the network into logical groups. Furthermore, the trust level of each logical group is calculated using entropy weight method and the local trust value of each node is updated periodically. Besides, the proposed Trust-Doe model able to detect malicious nodes but exhibits several limitations such as higher level of energy consumption and unable to defend other type of attacks such as Bad mouth, On-Off and Denial of service (Dos). Moreover, accurate detection of malicious node is another challenge which lacks in the proposed model. Nonetheless, the proposed Trust model should be attack resistant with optimal level of energy consumption. Figure 1 summarizes the various type of trust-based security estimation mechanisms deployed in WSNs.

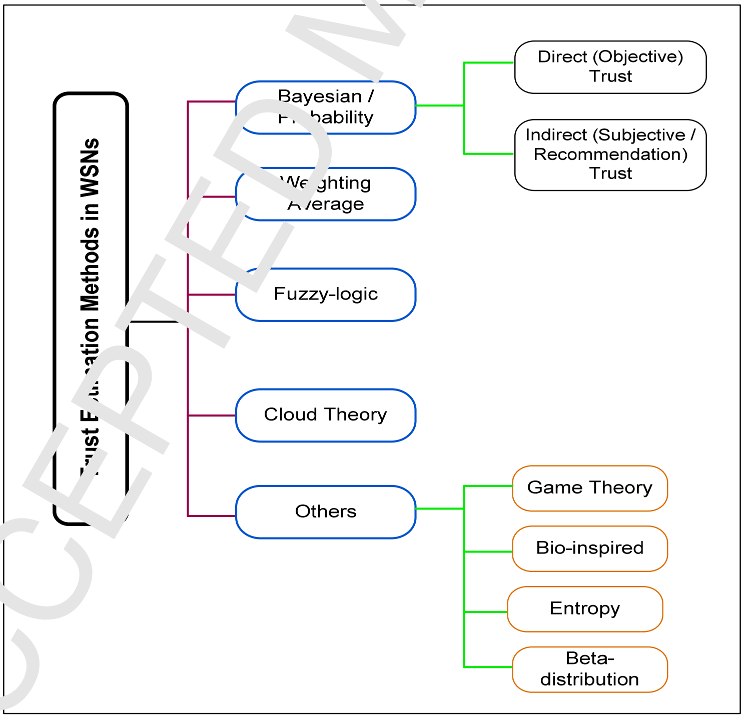

Figure 1: Trust Estimation Mechanisms in WSN

The literature review exposes comprehensive analysis of various trust models with the ability to defend attacks using direct and in-direct trust including other trust calculation metrics and network deployment. The proposed BTEM is partially motivated by those related works discussed above and summarized in Table 1. However, there are some differences as compared to already proposed approaches. BTEM estimates the trust level through sent, received and transit packets using direct observation and in-direct recommendation. Moreover, malicious nodes are not only isolated but various attacks are considered too not like the works in [25,26] where the trust values are based on either direct communication or only relying on in-direct interaction. Besides, some other studies [20-24] combine various trust metrices but forget to incorporate the resource constraint nature of sensor nodes due to algorithm complexity and higher energy consumption which not only affects the network reliability but increases delay. Based on the findings of the related literature the proposed BTEM is able to isolate the malicious nodes with resistance against On-Off, Bad-mouth and Denial of Service (DoS) attacks up to certain extent while increased in the network throughput and improves network reliability. The comparison of various trust-based security related work is summarized in Table 1.

Table 1: Comparison of existing trust models for WSNs

Trust models	Trust mechanism employed	Trust evidence collected	Attacks defended	Trust Estimation Method			Trust ca	
				Distributed	Centralized	Cross-Layer	Direct Trust	In-direct Recommend Trust
B-Trust [15]	Bayesian	Data packets	Sybil, Collusion	√	×	×	√	√
GTMS [16]	Weighing	Data packets	Malicious nodes	×	√	×	√	×
PLUS [17]	Weighing	Data packets	Modification, DoS	√	×	×	√	√
RFSN [18]	Weighing	Weighing	Bad-mouth, ballot stuffing, Identity attack	√	×	×	√	×
NBBTE [19]	Belief Theory	Neighbor nodes interaction	None	√	×	×	√	√
ReTrust [20]	Weighing	Data packets	On-off, bad-mouth		√		√	√
ARTMM [21]	Fuzzy, Weighing	Neighbor nodes interaction	Selective forwarding, Data modification, DoS, On-off, bad-mouth	√	×	×	√	√
EDTM [22]	Subjective, Weighing	Data packets, neighbor nodes	Selective forwarding, data forgery, DoS, On-off,	√	×	×	√	√

		interaction	Good, bad-mouth					
TruFix [23]	Fuzzy	Data packets	Blackhole, rushing, Sybil	×	×	√	√	×
TMC [24]	Cloud Theory, Weighing	Data packets	Selective forwarding, Dos, On-off, Good, bad-mouth	√	×	√	√	√
AF-TNS [25]	Activation Function	Data packets	None	√	×	×	√	×
Trust-Doe [26]	Entropy	Data packets	Collusion	√	×	×	√	√

In the light of aforementioned issues, this research proposes a belief based trust evaluation mechanism (BTEM malicious network node responsible for false reporting but also improves the network throughput, performance and

3 PROPOSED MODEL

3.1 The Design of BTEM

In this section, we discussed the detailed design of proposed Belief based Trust Evaluation Mechanism (BTEM). BTEM calculates the trust using direct interactions and in the form of recommendation from neighboring nodes. The following subsection discuss the components of BTEM and the notations which are used in these components are described in Table 2.

Table 2: Abbreviation and their meanings

Abbreviation	**Meaning**
TP	Traffic Profiles
TMM	Traffic Monitoring Module
TE	Trust Estimator
TR	Trust Receiver
PRE	Packet Received Evaluation
PSE	Packet Sending Evaluation
TPE	Transit Packet Evaluation
DTEM	Direct Trust Evaluation Mechanism
ITEM	In-Direct Trust Evaluation Mechanism
MN	Malicious Node
O | E	Occurrence | Evidence
P (E)	Normalizing Constant
R_{ij}	Data packet received
D_{ij}	Total drop packets
TV | J	Probability of Trust value
P (J)	Prior Probability

3.1.1 Components of BTEM

Belief based Trust Evaluation Mechanism (BTEM) consists of three modules. The first module is Traffic Monitoring Module, which observes packet forwarding behavior of neighboring nodes by exchanging request and response packets along with other traffic type information about nodes in form of traffic profiles (Tp). Moreover, the second module is the Trust Evaluation Module used to evaluate direct and in-direct trust of sensor nodes which is based on the past interactions such as send, receive and transit traffic profiles and forward these information to decision maker module (dm), for further action which in turn check node trust level against predefine threshold value, whether or not the value is greater or equal to threshold, then the node is categorized as trusted or if the node value is less then threshold then it is detected as malicious node hence isolated. Figure 2 represents the block diagram of the design of BTEM.

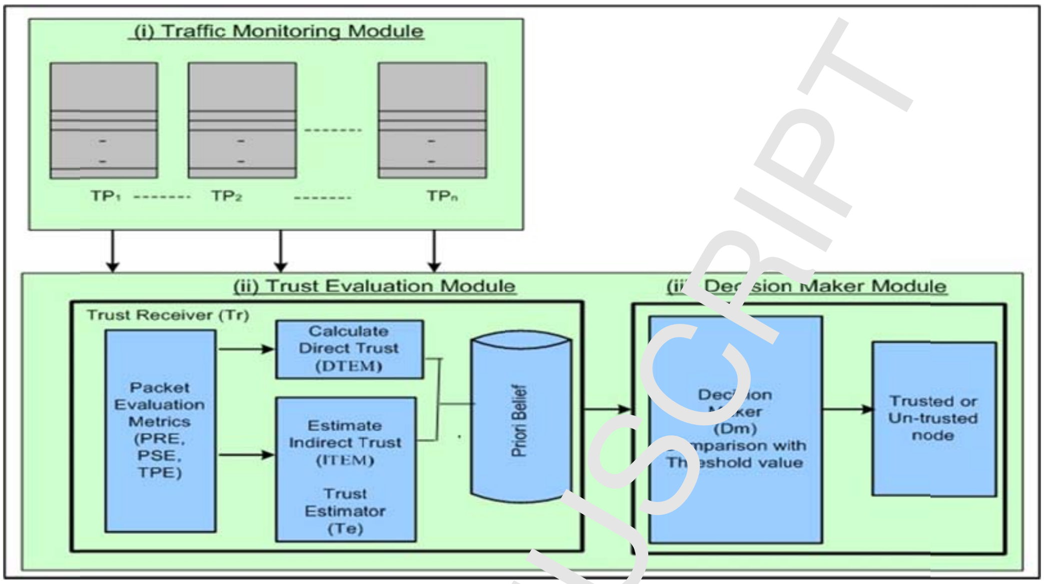
(i) Traffic Monitoring Module
TP₁ ------- TP₂ ------- TPₙ
(ii) Trust Evaluation Module
(iii) Decision Maker Module
Trust Receiver (Tr)
Packet Evaluation Metrics (PRE, PSE, TPE)
Calculate Direct Trust (DTEM)
Estimate Indirect Trust (ITEM)
Trust Estimator (Te)
Priori Belief
Decision Maker (Dm) Comparison with Threshold value
Trusted or Un-trusted node

Figure 2: Trust Estimation Mechanism of BTEM

3.1.2.1 Traffic Monitoring Module

As shown in Figure 2, Traffic Monitoring Module observe the packet forwarding behavior of neighboring nodes through the exchange of Request and Response control packets which consists of Traffic Profiles (Tp), maintained at each node and contains three types of traffic information: (i) Sent Data Packets, (ii) Received Data Packets and (iii) Transit Data Packets. In addition, the stored information consists of total packets transmitted between the nodes including source and destination. The working mechanism of Traffic Monitoring Module of the proposed mechanism is discussed as follows. It is assumed that nodes i, j and k are neighboring nodes that participate in packet forwarding mechanism at one-hop neighbor and in the transmission range of each other. Figure 3 shows the network topology where data packet streams are evidence of packet forwarding behavior that a node utilizes in calculating direct and in-direct trust.

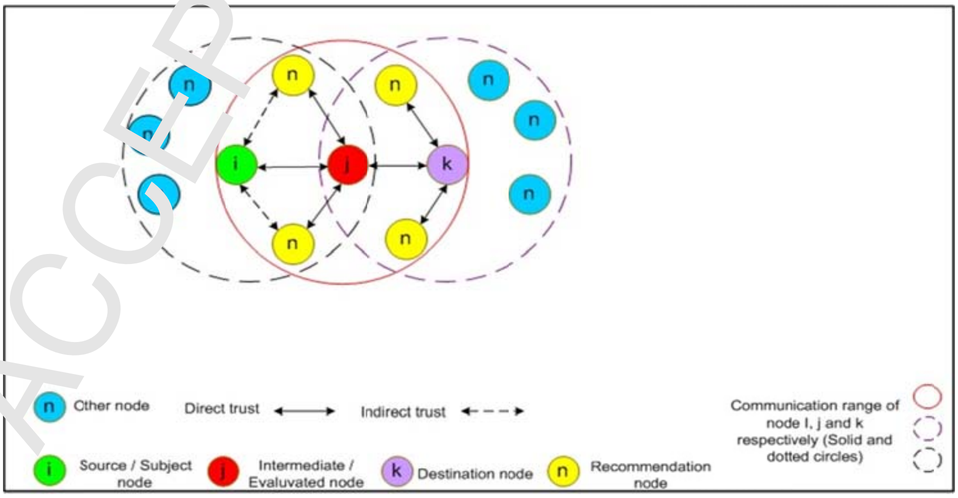

Figure 3: BTEM – Network Topology Scenario

The direct trust calculation mechanism is done through transmitted data packets from node 'i' to 'j' at time 't' and further determines if the node 'j' forward these packets onwards to node 'k'. The trustworthiness level of the node is evaluated through packet sending, receiving and transit information, which are stored in traffic profiles (Tp), and maintained at each node which are:

I. Packet Received Evaluation $PRE_{ij}(t)$, the number of packets node j received from node i in the time period of t.

II. Packet Sending Evaluation $PSE_{ij}(t)$, the number of packets node i send to node j in the time period of t.

III. Transit Packet Evaluation $TPE_{ij}(t)$, the number of packets node i send to node k through intermediate node j in the time period of t.

The calculation of trustworthiness is based on the probability of trust values. The Traffic Monitoring Module, at each neighbouring node helps in obtaining the true behaviour (node 'i' to 'k') by observing the packet forwarding behaviour of node j. The node 'i' can determine the trustworthiness level of node 'j' through its packet forwarding ratio to node 'k' and this could be verified through shared traffic profile (Tp) of node 'j' and if this ratio matches the send packet by node 'i' through node 'j', then node 'i' considers node 'j' as trustworthy. Moreover, node 'i' also verifies packet forwarding behaviour of node 'j' from neighbouring nodes in form of indirect trust or recommendation. However, with the passage of time the more traffic flows are evidenced, which may update the probability of trustworthiness while trust relationship among nodes may also change due to instability of communication channel. Therefore, the Probabilistic Bayesian Estimation Theory is applied on that trust level to validate the trustworthiness of the node. The trust level is evaluated based on three parameters: (i) Packet Received Evaluation (PRE), (ii) Packet Sending Evaluation (PSE) and (iii) Transit Packet Evaluation (TPE).

3.1.2.2 Trust Evaluation Module

Trust evaluation module is responsible for evaluating trustworthiness value of each communicating node through its packet forwarding, receiving and transit packet behaviour and estimates the probability of a node whether it is malicious or trustworthy. A node is declared as trustworthy if it forwards all the packets to intended destination node and these information's are recorded in traffic profile which is then shared with other neighbouring nodes as directly or indirectly. Similarly, node is considered as malicious if it intentionally drops some or all the packets and record wrong information in the traffic profile by indicating correct number of received and forwarded packets. The Trust Evaluation Module is further divided into three sub-components to critically examine and evaluate the results, i.e. (i) Trust Receiver (ii) Trust Estimator (iii) Positivity Test based Decision Maker. These components are discussed in the following sub-sections.

A. Trust Receiver (TR):

The Trust Receiver (TR) consists of three modules (i) Traffic Evaluation Metrics, (ii) Direct Trust Evaluation Mechanism (iii) Indirect Trust Evaluation Mechanism. As per Figure. 2, the composing elements of traffic evaluation metrics are:

1. Packet Received Evaluation PRE:

Packet received evaluation represents the ratio of packets received at the node 'k' from sender node 'i' in the time period of t. The network may encounter packet loss due to the presence of malicious nodes. Depending upon the distance from the sender node to receiving node, there can be multiple malicious nodes and accordingly, the loss of packets can also be critical. The number of packets that were received by the receiver from sender node is referred as direct receiving report. In equation 1, the PRE shows the ratio of the packets received.

$$PRE_{ij}(t) = \frac{Pr_{ij}(t) - Pr_{ij}(t-1)}{Pr_{ij}(t) + Pr_{ij}(t-1)} \qquad (1)$$

Where $\mathrm{Pr}_{\mathrm{ij}}(\mathrm{t})$ represents the number of packets received from sender to receiver in the time interval 't'. The two consecutive time intervals are taken into consideration to describe the state of the evaluated node more accurately, and the denominator is used for normalizing the results.

2. Packet Sending Evaluation:

Packet sending evaluation represents the number of packets sent from node 'j' to node 'k' are monitored by node 'i' in the time period of 't'. Also, the packets that an intermediate node forwards successfully to the next node cannot be monitored directly by the sender but any node in the communication range can receive the packets if they are tuned on the same channel and their receiver (Rx) is turned on. Therefore, the sender can still monitor the number of forwarded packets sent by intermediate node. The calculation mechanism of $\mathrm{Ps}_{\mathrm{ij}}(\mathrm{t})$ at intermediate node as well as sender node is made as:

$$PSE_{ij}(t) = \frac{Ps_{ij}(t)}{Ps_{ij}(t) + PRT_{ij}(t-1)} \qquad (2)$$

In the above equation, $\mathrm{Ps}_{ij}(t)$ represents the packet needs to be transmitted, but there are some packets that require retransmission as these packets are not received. The reason of not receiving and retransmitting can be due to the lossy channel or the presence of malicious node. In this research, presence of malicious node is assumed, therefore, retransmitted packets are also taken into consideration and represented as with PRT_{ij} in Equation 2.

3. Transit Packet Evaluation:

Transit packet evaluation represents the number of packets that sender 'i' sends to receiving node 'k' through some intermediate node(s) in the time period of t. In multi-hop environment, it is quite difficult that a node can directly communicate with a receiving node. This communication can be possible by involving the intermediate node(s). Once the node 'j' updates its traffic profile and update to the 'i' node, after verification, the information becomes true then this is treated as trusted as well as un-trusted. The calculation mechanism of $\mathrm{TPE}_{ij}(t)$, at intermediate node and receiving node is made as:

$$TPE_{ij}(t) = \frac{TP_{ij}(t) - TP_{ij}(t-1)}{TP_{ij}(t) + TP_{ij}(t-1)} \qquad (3)$$

Where TP_{ij} represents actual number of transmitted packets which are sent from node 'j' to 'k', transit and actual receive packets at intermediate node and shared between node 'j' to 'i'.

B. Direct Trust Evaluation Mechanism (DTEM):

In each pair of communicating nodes, different number of packets travel in different time intervals and their successfulness varies in each interval. This variation has influence on the next interval also, therefore, in order to ensure the effectiveness of DTEM, this variation is also considered by including a Trustworthiness action parameter T, which considers the effect of previous intervals as shown in the Equation 4.

$$T_{ij}^{direct} = \frac{R_{ij}(t)/(D_{ij}(t)+R_{ij}(t))}{R_{ij}(t-1)/[D_{ij}(t-1)+R_{ij}(t-1)]} \qquad (4)$$

Where $\mathrm{R}_{ij}(t)$ is the number of the data packets received at a specified time interval, whereas $\mathrm{D}_{ij}(t)$ is the total of dropped packets during that transmission so, the overall evaluation on the basis of direct trust, the $\mathrm{DTEM}_{ij}(t)$, is represented as:

$$\begin{aligned} DTEM_{ij}(t) =\ & T\ x\ PIT(t)\ x\ [w_1 \times \left(1 - \left|PRE_{ij}(t)\right|\right) \\ & + w_2 \times \left|PSE_{ij}(t)\right| + w_3 \times \left(1 - \left|TPE_{ij}(t)\right|\right) + \left(1 - PIT(t)\right) \times DTEM_{ij}\ (t-1) \end{aligned} \tag{5}$$

In the above equation, Packet Interval Time PIT(t) is the time interval of a packet received by node 'i' or at the intermediate node 'j' at time t. T is the action parameter which consider the effect of time intervals. Similarly, weighting algorithm is used for the process of decision making where each factor influence in obtaining the final result. The overall trust value of each node participating in the network is determined by combining direct and in-direct trust and by categorizing with different weights. The incorporation of different weights in the proposed mechanism is based on their immense influence to reduce the probability of false recommendation offered by other nodes. Hence, $\mathrm{w}_1, \mathrm{w}_2, \mathrm{w}_3$ are trust's values that should satisfy $\mathrm{w}_1 + \mathrm{w}_2 + \mathrm{w}_3 = 1$ [27, 28]. In this research, all the weights are equally treated, however, for different practical applications different weights can be assigned to w1, w2, and w3 based on the precedence of PRE, PSE, and TPE.

C. In-direct Trust Evaluation Mechanism (ITEM):

Indirect trust is observed when prior trust relationship is not ascertained by two nodes via packets exchange or any other form of interaction. To calculate the indirect trust between sensor node 'i' and evaluated node 'k', where the nodes n1, n2, n3, n4 are the common neighbours (recommendation nodes as shown in Figure 3 above) of 'i' and 'k', the direct trust values (DTEM) of sender node 'i' to all neighbouring node 'n' and from all neighbouring node 'n' to receiver node 'k' are collectively used as in-direct trust estimation (ITEM).

Trust transitivity is major characteristics in the formation of trust where, if node 'a' trust on node 'b', and node 'b' trust on node 'c', then the node 'a' indirectly trusts on node 'c'. Similarly, trust could be intransitive, i,e, if node 'a' trusts on node 'b' and node 'b' trusts on node 'c', this does not necessarily imply on node 'a' to trust on node 'c'. Moreover, this intransitive trust does not rule out the possibility of the transfer of trust information [9, 29]. Each time the $\mathrm{DTEM}_{\mathrm{nj}}$ calculated by node 'n' for node 'j', is conveyed to node 'i' as a recommendation of trust of node 'j'. Therefore, on each update of a recommendation, the probability of node 'j' being trustworthy or malicious updated accordingly. The incorporation of indirect trust information is essential in a trust mechanism due to its benefits in offering information regarding unrecognized nodes by the evaluating node. In contrast, the mechanism can be assumed vulnerable as the involvement of particular information create untrustworthy suggestions. Therefore, it is essential to explore the trustworthiness of the information for reducing the effects of false positive.

In order to determine the intensity of this belief, the Bayesian estimation approach is employed. This estimation is based on the probability of an incident using the evidence in hand. However, because each time the evidence is updated based on the number of dropped packets, therefore, the posterior probability of any node being malicious or trustworthy is also updated periodically. The posterior probability is a measure of belief that updates in response to evidence. The Bayesian estimation is based on prior probability, therefore, each time the new probability is calculated, it is also stored in the database for reusage as a prior probability in the next round. Mathematically, the Bayesian theorem is represented in Equation 6.

$$P(O \mid E) = \frac{P(E\mid O)\, P(O)}{P(E)} \qquad (6)$$

The conditional probability is given by (O | E) , where O is the occurrence of an event and represents the evidence and probability of E which is assumed to be true if it is provided, similarly, the P(E| O) represents the probability of E where O is assumed true. The probabilities of O and E are represented separately as P(O) and P(E) which are independent and where P(O) is representing prior probability and normalizing constant is represented by P(E) [30]. The problem of trust estimation in the proposed approach is mapped to Bayesian estimator using the Equation 7 as represented below:

$$P(J\ |TVnj) = \frac{P(TVnj\ |\ J\ )\ P(J\ )}{P(TVnj)} \qquad (7)$$

In the above equation, probability of trust for evaluated node 'j' is calculated, provided the direct trust of evaluated node 'j' by the neighbouring node 'n'. The (TV | J) represents the probability of trust value, when it is assumed that node 'j' is trustworthy. The P(J) represents the prior probability which was found in the previous round. The P(TVnj) represents the normalization factor that is the over all probability in all the circumstances. The Equation 8 is the level of trustworthiness of evaluated node 'j' by one of the common neighbours of a sender node 'i'. There can be a different number of neighbouring nodes to accommodate the recommendation for all the neighbors. Equation 8 computes the indirect trust (ITEMij).

$$ITEMij \ = \ \frac{\sum_{n=0}^{N} P(j\ is\ trustworthy\ |\ Trust\ Value\ nj)}{N} \qquad (8)$$

To accumulate the direct trust and indirect trust, both the trust values of DTEM and ITEM calculated by Equations 7 and 8 respectively are used in Equation 9.

$$Total\ Trust = \ DTEMij + ITEMij \qquad (9)$$

It can be seen from Figure 2, that the various components of proposed BTEM is discussed which reflects the working mechanism of the proposed approach.

3.1.2.3 Decision Maker (Dm) Module

The output from Trust Evaluation Module forwards the node to decision maker (Dm) module where probability of a node as malicious or non-malicious is compared against the threshold value which range from 0 to 1. Previously, many researches have used the concept of trust using pre-defined values as (1 and 0), where 0.5 is set as a primary trust value. Therefore, in this research the threshold value is set at 0.5. Hence, the trusted node is having the probability greater than 0.5 and if the value approaches to 1, then the node is treated as most trustworthy. Similarly, the probability of the node having less than 0.5, value is considered as malicious or compromised node.

4 IMPLEMENTATION OF PROPOSED MECHANISM

The algorithm of the proposed approach takes the traffic profiles as input and bifurcate them as sent, received and transit packets. In line 1-3, the averages of all the three types of packets are calculated based on periodic intervals. The probability of a node being malicious or non-malicious is calculated in line 4 based on Bayesian estimation theory as discussed in Section 3.1.2.2. In line number 5 and onward, the calculated probability is evaluated against the threshold to mark the node as trusted or un-trusted.

```
Algorithm 1: Node Reputation calculation
Input: Traffic Profiles (Pr, Ps, Tp)
Output: detection as trusted / un-trusted node
1:  $PRE$ = calculate average received packets in the last interval
2:  $PSE$ = calculate average sent packets
3:  $TPE$ = calculate average transit packets in the last interval
4:  $P(\mathrm{MN}|PSE) = \frac{P(PSE|\ \mathrm{MN})\ P(\mathrm{MN})}{\mathrm{P\ (PSE\ )}}$
5:  if $P(\mathrm{MN}|PSE)\ > \mathrm{Th}$
6:  Then mark as Trusted
7:  Else
8:  Mark as Un-trusted
9:  Update database for prior probability
10: end if
```

The proposed Belief based Trust Evaluation (BTEM) Mechanism evaluates the integrity and trustworthiness level of nodes in a network and maintains the trusted environment through identification of malicious nodes responsible for causing internal attacks such as Bad-mouth, On-off, Denial of Service (DoS) and false reporting which hinder in reliable data delivery. Therefore, to determine the current trust level of the node, the proposed (BTEM) mechanism designed in a way that copes with false reporting and evaluates the trust level of each node by incorporating direct trust, and in-direct trust in the form of recommendation by evaluating received data packets, sent data packet and through transit packet information. The flow chart of the proposed BTEM mechanism is given in Figure 4.

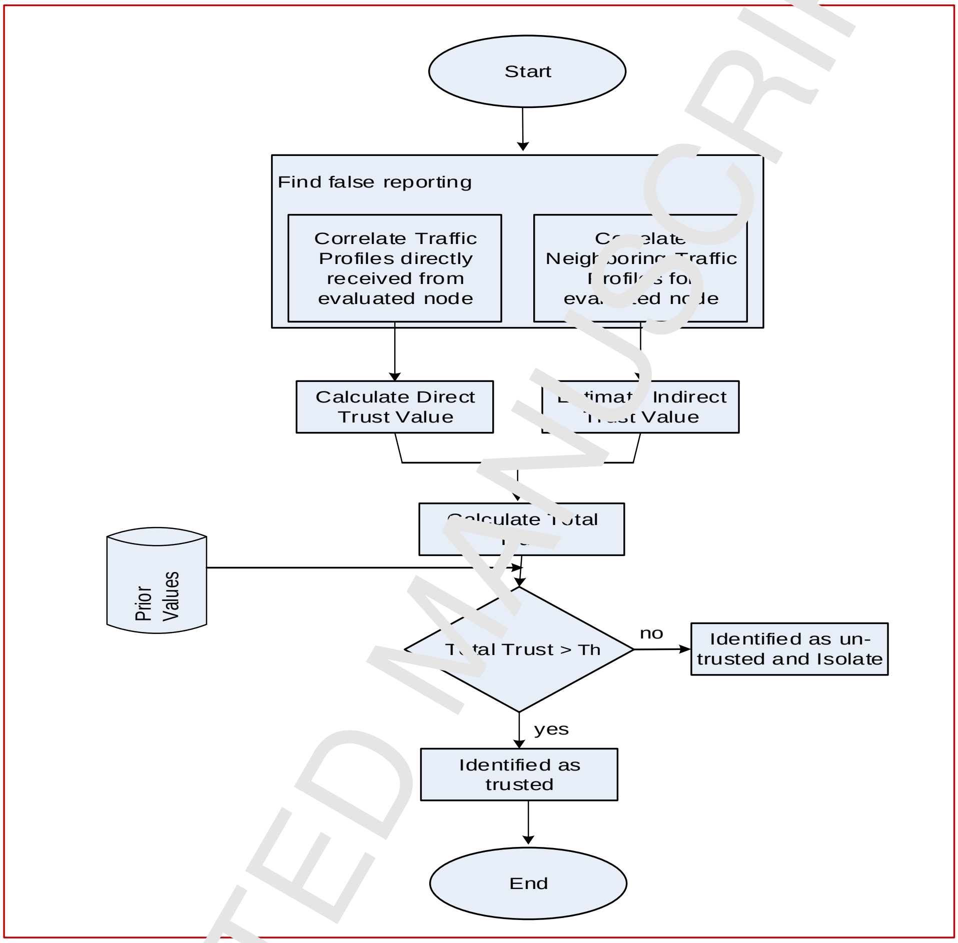
Start
Find false reporting
Correlate Traffic Profiles directly received from evaluated node
Correlate Neighboring Traffic Profiles for evaluated node
Calculate Direct Trust Value
Estimate Indirect Trust Value
Calculate Total
Prior Values
Total Trust > Th
no
Identified as un-trusted and Isolate
yes
Identified as trusted
End

Figure 4: Flow diagram of the proposed mechanism

The focus of this study is to identify and isolates the malicious node and to explore the impact on the performance of the network.

4.1 Simulation Parameter

In order to ascertain the performance of the proposed mechanism, the BTEM is tested in a simulation by implementing it in discrete event simulator, OMNET++. The sensor nodes are randomly deployed in the field size of 100 x 100 m with the transmission range of nodes are kept at 20 m [19]. The sensor nodes and sink nodes are deployed statically with same initial energy, computation and storage capacity. The simulation time varies between 200 to 1000 Sec for different experiments. Initially all the nodes behave as trustworthy however, with the passage of time, some of the nodes behave as malicious. The malicious nodes are simulated through Bad-mouth (BM), On/Off and Denial of Service (DoS) attacks. In order to detect the malicious nodes their trust updating time period is set to 40 Sec [22]. Therefore, on average in this experiment for every node the trust value is updated 25 times. To evaluate the trustworthiness of nodes, which ranges between 0 and 1, the trust value of 0.5 is set as threshold. In addition to obtaining a trust value, threshold value is used to differentiate between trustworthy and malicious node and avoids false accusation. The traffic flowed on the network is of CBR type and packet size is set to 50 bytes [22, 31, 32]. Due to reactive and on-demand nature AODV is considered as a baseline routing protocol [33-35]. Table 3 enlists the other simulation parameters.

Table 3: Simulation Parameters

Parameters	**Values**
Field Size	100m x 100m
Node deployment	Random
Simulation Time	200 – 1000 seconds
Traffic Type	UDP
Packet Size	50 Bytes
Physical Standard	IEEE 802.15.4
Traffic Load	CBR
No. of nodes	10,20,30,40, 50

4.2 Results and Discussion

Impact of Level of Trustworthiness

In the first scenario the level of trust is analysed in the presence of malicious sensor nodes. As it can been seen from Figs. 5 and 6, that the level of trustworthiness of the proposed BTEM mechanism is increasing as contrast to AF-TNS [25] and Trust-Doe [26], with the passage of time, the proposed approach gets a higher level of trustworthiness due to its predictive behaviour on analyzing false reporting and accurately identifying the malicious nodes.

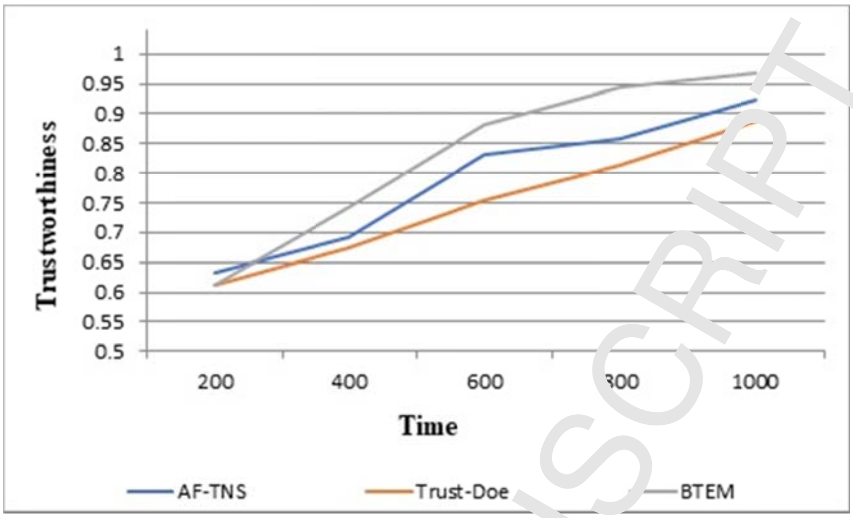

Figure 5: Trustworthiness with advancement in time

The ratio of malicious sensor nodes varied from 10% to 50% of the whole scenario with an average increase of 10% as shown in Figure 6. For certainty, the observation of experiments was taken at different timing of the simulation varying from 200 Sec. to 1000 Sec.

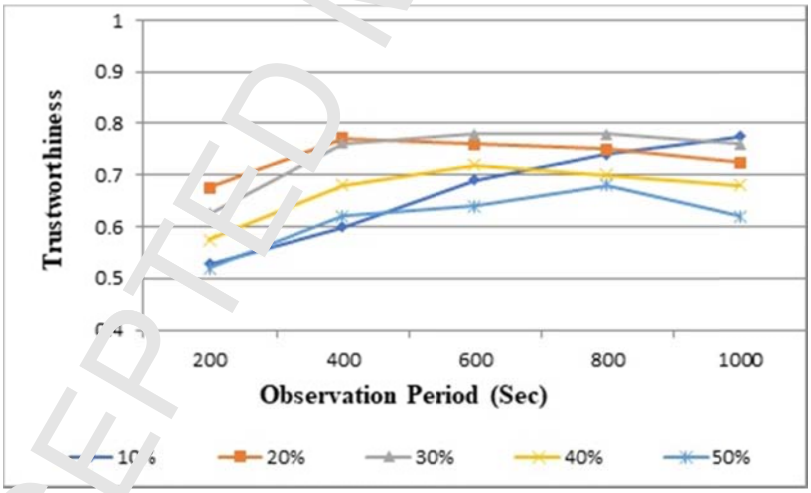

Figure 6: Trustworthiness as malicious sensor nodes increase

In the third scenario of the simulation, Bad-mouth, On-off and Denial of Service (DoS) attacks are simulated with varying number of malicious nodes 10% to 50% with an increment of 10%. Figure 7 represents a rationale of On-off, Bad-mouth and Denail of Service (DoS) attacks and their effect on trustworthiness level. The said graph only depicts the observation values at 200 seconds.

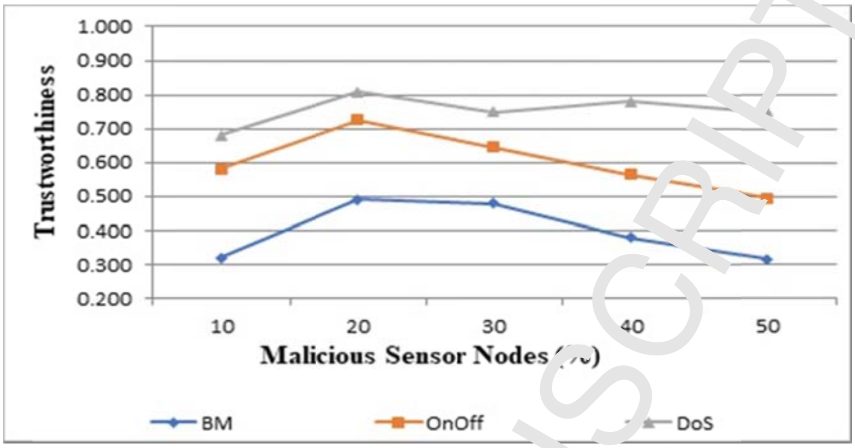

Figure 7: Trustworthiness proportional malicious sensor nodes for different attacks

The On-Off attack directly affects the trust management system where malicious node behaves alternatively between normal node to malicious and remain undetected while degrading the network performance [36]. The results indicates that the proposed BTEM effectively detects the altering behaviour of nodes. The early detection and isolation of malicious nodes allowed in saving the bandwidth, transmission power and energy that is required for re-transmission of data packets [37]. Similarly, it is observed that the two other simulated Bad-mouth and Denial of Service (DoS), attacks are effectively deteced by the proposed mechanism due to the ability in the selection of trustworhty node and including the consideration of false positive rate of trust evaluation. To evaluate the effectiveness of the proposed algorithm attacks are simulated using three layers (Application, Physical and Network layer). Moreover, the following Table 3, presents the complete observation period which is used in the simulation against Bad-mouth, On-off and Denial of Service (DoS) attacks.

Observation Period (Sec)	Percentage of Malicious Sensor Nodes											
	10			20			30			40		
	BM	On/Off	DoS	BM	On/Off	DoS	BM	On/Off	DoS	BM	On/Off	Do
200	0.320	0.580	0.680	0.490	0.725	0.810	0.480	0.645	0.750	0.380	0.565	0.7
400	0.470	0.610	0.720	0.610	0.823	0.880	0.580	0.835	0.870	0.490	0.690	0.8
600	0.570	0.690	0.810	0.590	0.810	0.880	0.610	0.840	0.890	0.580	0.730	0.8
800	0.630	0.740	0.850	0.580	0.800	0.870	0.620	0.830	0.890	0.570	0.710	0.8
1000	0.670	0.764	0.890	0.560	0.785	0.830	0.570	0.830	0.880	0.560	0.680	0.8

Table 4: Effect on trustworthiness in comparison with different attacks

Impact of Trust Detection Rate

Figure 8 shows the number of malicious sensor nodes in the network which influenced on trust detection rate. The proposed BTEM mechanism successfully detects the malicious nodes. Simulation is conducted using varied numbers of malicious nodes from 10% to 50% of the whole topology with an increment of 10%. The BTEM is compared with AF-TNS [25] and Trust-Doe [26]. As shown in Figure 8 the detection rate of malicious nodes is higher than its counter parts 8% and 28% respectively, which is due to the consideration of prior knowledge in the form of sent, receive and transit data packets for trust evaluation. Moreover, as the number of neighboring nodes increased, the probability of detecting the malicious node is slightly decreased which is due to the result of increased number of false reporting which gradually increases false positive ratio between the monitoring nodes.

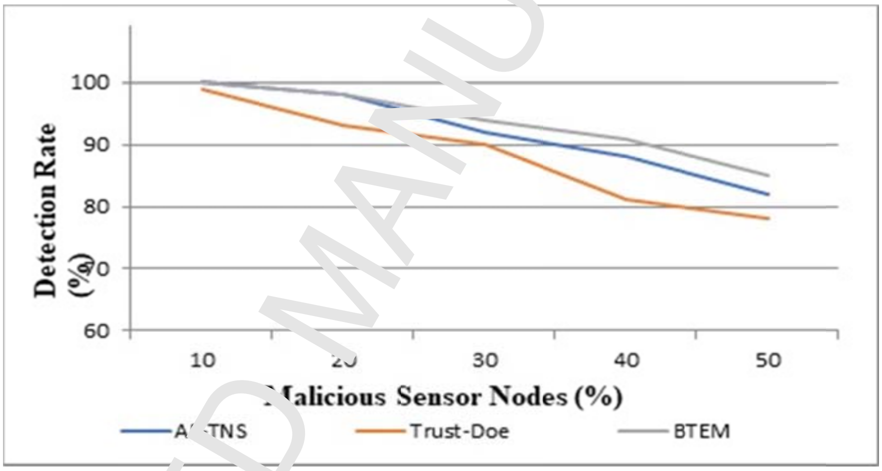

Figure 8: Influence on detection rate as malicious sensor nodes increase

Impact of Detection Accuracy

Figure 9 shows the detection accuracy metric which indicates the accurate detection percentage (%) of proposed BTEM mechanism with a minimize number of false positive recommendations. The detection accuracy of the proposed BTEM is 25.33% and 64.33% respectively. It is observed that the detection accuracy level of the BTEM is better than the AF-TNS [25] and Trust-Doe [26] in comparsion respectively, which is due to the consideration of trust establishment and increased cooperation between nodes with lesser number of packet drop rate

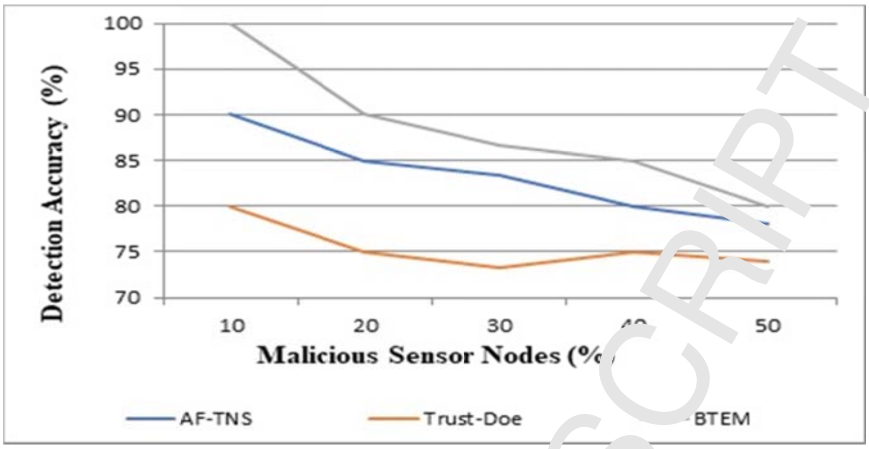

Figure 9: Detection Accuracy

Impact of False-positive Rate Detection

The proposed BTEM detects the false positive rate under different attacks. Figure 10 shows the False positive detection rate of BTEM which is 17.33% and 36.33% respectively. In addition, the detection of false positive rate in the proposed BTEM is better than the AF-TNS [25], and Trust-Doe [26], which is due to attacks that have very little influence on trust values of trustworthy nodes but on the other hand false positive rate influence is much higher on malicious nodes in AF-TNS and Trust-Doe schemes.

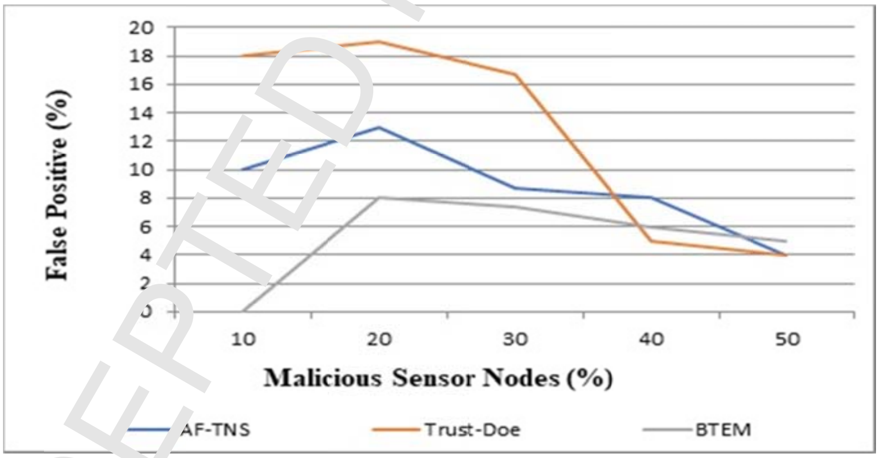

Figure 10: False Positive Rate

Impact of Residual Energy

Energy consumption of the node influence the network lifetime. The higher is the energy consumption the shorter will be the life of the network. Figure 11 shows the node residual energy consumption against the malicious node which varied from 10% to 50%. The average energy consumption of nodes in the proposed BTEM is compared with AF-TNS [25] and Trust-Doe [26]. The result shows that the proposed mechanism preserves better energy level than AF-TNS and Trust-Doe which is due to increased trustworthiness level and lesser energy consumption among nodes while the other schemes exhibits higher energy consumption due to increased overhead and communication cost.

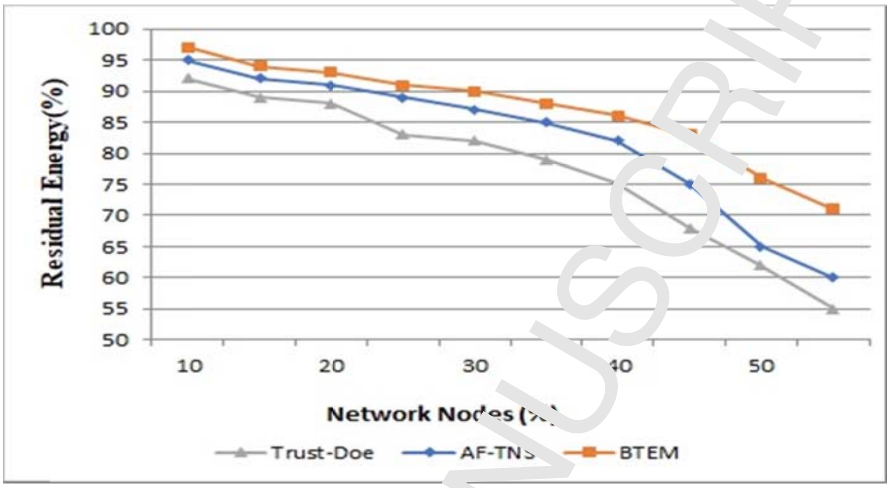

Figure 11: Energy Consumption Comparison

Impact of Average Throughput

In this experiment the effect of throughput is analyzed by exhibiting the network in the presence of malicious nodes. Figure 12 represents the comparison of average throughput. The graph shows that, BTEM performance is better with lesser delay when there are 10% malicious nodes as compare to AF-TNS [25] and Trust-Doe [26]. Similarly, when the malicious nodes increase from 20% - 50%, BTEM throughput is still higher than the AF-TNS and Trust-Doe, because the proposed mechanism consider both trustworthiness and energy level of the node.

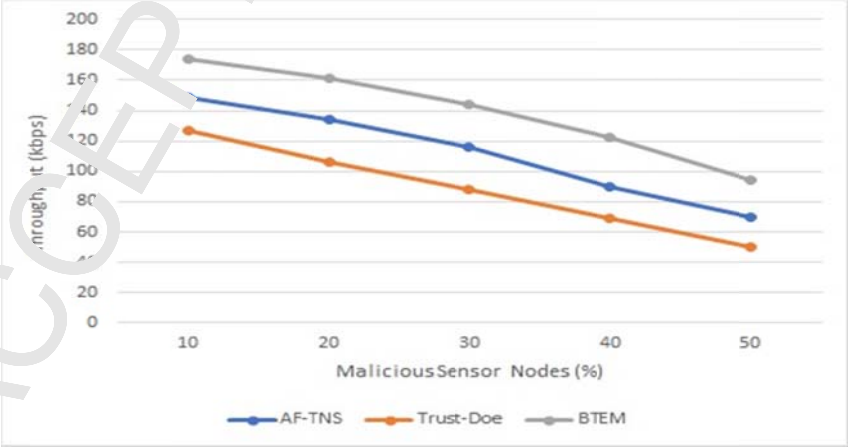

Figure 12: Average Throughput

Impact of End-to-End Delay

In this scenario, average network delay is analyzed in the presence of malicious nodes which varies from10% to 50% of the whole topology with an increment of 10%. Figure 13 represents the graph, which shows the performance comparison level, it is observed that BTEM and AF-TNS encounter almost similar delay level in the presence of 10 % malicious nodes. However, when the malicious node increases to 20% and onward the delay between AF-TNS [25] and Trust-Doe [26] started increasing whereas, BTEM behaves slightly different from the both (AF-TNS and Trust-Doe), due to the selection of trustworthy nodes with higher energy level.

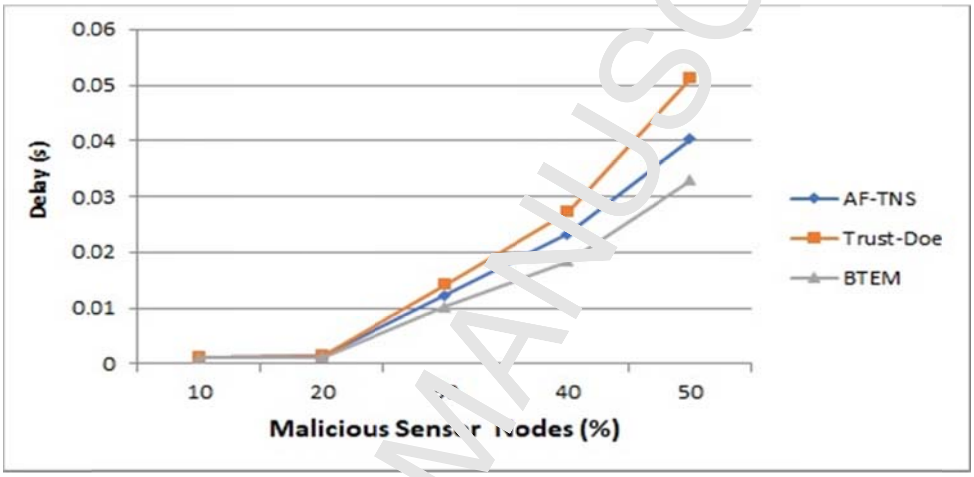

Figure 13: End-to-End Delay

5 CONCLUSIONS AND FUTURE WORK

Securing WSNs using trust establishment mechanism is a promising approach. In this paper, an efficient Belief based trust evaluation mechanism (BTEM) is proposed which defends against the malicious node and internal attacks. Bayesian estimation is applied in gathering direct and In-direct trust values of the sensor nodes which further considers the correlation of the data collected over the time and then used it further in the selection of trustworthy node for data forwarding. Simulation results prove that the proposed mechanism not only successfully identifies and isolates the malicious nodes to the certain extent but also improves the false-positive detection rate. So it can be conculuded that the propossed mechanism have better ability to defend against On-off, Bad-mouth and DoS attacks as compare to AF-TNS [25] and Trust-Doe [26] . In the future, the proposed mechanism improved further to include other type of malicious node attacks such as Sybil, selective forwarding and wormhole attacks.

ACKNOWLEDGEMENT

The authors would like to extend their appreciation to the Deanship of College of Technological Innovation (CIT) at Zayed University, Dubai for funding this research. Also, the authors would like to extend their appreciation for the Ministry of Education Malaysia in collaboration with Research Management Center at Universiti Teknologi Malaysia.

REFERENCES

1. Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc networks, 1(1), 175-192.
2. Yang K. Wireless sensor networks. Principles, Design and Applications. 2014.
3. Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.
4. Long, J., Dong, M., Ota, K., Liu, A., & Hai, S. (2015). Reliability guaranteed efficient data gathering in wireless sensor networks. IEEE Access, 3, 430-444.
5. Chakrabarti, A., Parekh, V., & Ruia, A. (2012, January). A trust based routing scheme for wireless sensor networks. In International Conference on Computer Science and Information Technology (pp. 159-169). Springer, Berlin, Heidelberg.
6. Stelios, Y., Papayanoulas, N., Trakadas, P., Maniatis, S., Leligou, H. C., & Zahariadis, T. (2009, May). A distributed energy-aware trust management system for secure routing in wireless sensor networks. In International Conference on Mobile Lightweight Wireless Systems (pp. 85-92). Springer, Berlin, Heidelberg.
7. Karlof, C., & Wagner, D. (2003, May). Secure routing in wireless sensor networks: Attacks and countermeasures. In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on (pp. 113-127). IEEE.
8. Feng, R., Che, S., Wang, X., & Yu, N. (2013). Trust management scheme based on DS evidence theory for wireless sensor networks. International Journal of Distributed Sensor Networks, 9(6), 948641.
9. Momani, M. M. (2008). Bayesian methods for modelling and management of trust in wireless sensor networks (Doctoral dissertation).
10. Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys & Tutorials, 14(2), 279-298.
11. Ishmanov, F., Kim, S. W., & Nam, S. Y. (2014). A secure trust establishment scheme for wireless sensor networks. Sensors, 14(1), 1877-1897.
12. Yan, Z., & Holtmanns, S. (2008). Trust modeling and management: from social trust to digital trust. In Computer security, privacy and politics: current issues, challenges and solutions (pp. 290-323). IGI Global.
13. Zhou, H., Wu, Y., Feng, L., & Liu, D. (2016). A security mechanism for cluster-based wsn against selective forwarding. Sensors, 16(9), 1537.
14. Momani, M., & Challa, S. (2010). Survey of trust models in different network domains. arXiv preprint arXiv:1010.0168.
15. Quercia, D., Hailes, S., & Capra, L. (2006, May). B-trust: Bayesian trust framework for pervasive computing. In International Conference on Trust Management (pp. 298-312). Springer, Berlin, Heidelberg.
16. Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2009). Group-based trust management scheme for clustered wireless sensor networks. IEEE transactions on parallel and distributed systems, 20(11), 1698-1712.

17. Yao, Z., Kim, D., & Doh, Y. (2008). PLUS: parameterised localised trust management-based security framework for sensor networks. International Journal of Sensor Networks, 3(4), 224-236.
18. Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN), 4(3), 15.
19. Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. Sensors, 11(2), 1345-1360.
20. He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. IEEE transactions on information technology in biomedicine, 16(4), 623-632.
21. Han, G., Jiang, J., Shu, L., & Guizani, M. (2015). An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network. IEEE Transactions on Mobile Computing, 14(12), 2447-2459.
22. Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2015). An efficient distributed trust model for wireless sensor networks. IEEE Transactions on Parallel & Distributed Systems, (1), 1-1.
23. Umar, I. A., Hanapi, Z. M., Sali, A., & Zulkarnain, Z. A. (2017). Trufix: A configurable trust-based cross-layer protocol for wireless sensor networks. IEEE Access, 5, 2550-2562.
24. Jiang, J., Han, G., Shu, L., Chan, S., & Wang, K. (2017). A trust model based on cloud theory in underwater acoustic sensor networks. IEEE Transactions on Industrial Informatics, 13(1), 342-350.
25. AlFarraj, O., AlZubi, A., & Tolba, A. (2018). Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1-11.
26. Nie, S. (2017). A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. Cluster Computing, 1-10.
27. Rehman, E., Sher, M., Naqvi, S. H. A., Badar Khan, K., & Ullah, K. (2017). Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network. Journal of Computer Networks and Communications, 2017.
28. Ye, Z., Wen, T., Liu, Z., Song, X., & Fu, C. (2017). An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks. Journal of Sensors, 2017.
29. Lopez, J., Roman, R., Agudo, I., & Fernandez-Gago, C. (2010). Trust management systems for wireless sensor networks: Best practices. Computer Communications, 33(9), 1086-1093.
30. Iqbal, S., Abdullah, A. H., Ahmad, F., & Qureshi, K. N. (2017). Critical link identification and prioritization using Bayesian theorem for dynamic channel assignment in wireless mesh networks. Wireless Networks, 1-13.
31. Bao, F. (2013). Dynamic Trust Management for Mobile Networks and Its Applications (Doctoral dissertation, Virginia Tech).
32. Zahedi, A., & Parma, F. (2018). An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks. Peer-to-Peer Networking and Applications, 1-10.
33. Farooq, H., & Tang Jung, L. (2013). Energy, traffic load, and link quality aware Ad Hoc routing protocol for wireless sensor network based smart metering infrastructure. International Journal of Distributed Sensor Networks, 9(8), 697582.
34. Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. (2015). Security and performance enhancement of AODV routing protocol. International Journal of Communication Systems, 28(14), 2003-2019.
35. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2016). A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks, 22(5), 1505-1511.
36. Perrone, L. F., & Nelson, S. C. (2006, September). A study of on-off attack models for wireless ad hoc networks. In Operator-Assisted (Wireless Mesh) Community Networks, 2006 1st Workshop on (pp. 1-10). IEEE.

37. Tang, S., Shagdar, O., Yomo, H., Shirazi, M. N., Suzuki, R., & Obana, S. (2008, November). Layer-2 retransmission and combining for network coding-based forwarding in wireless networks. In Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on (pp. 1597-1602). IEEE.

Authors Bibliographic Details

1. Mr. Raja Waseem Anwar

Raja Waseem Anwar is currently registered as PhD student in the department of computer science at Universiti Teknologi Malaysia (UTM), Malaysia. He has received his MS Degree in Information Technology from PIMSAT- Karachi, Pakistan. His research interests includes Trust and Security in Wireless Sensor Networks ,Cyber-physical systems and IoT.

2. Dr. Anazida Zainal

Dr. Anazida Zainal has received her Ph.D from the department of Computer Systems and Communications in University of Technology Malaysia (UTM). Her research interest is in Information Security, Intrusion Detection Systems and Wireless Sensor Networks. She has published many papers in field of IDS and information security.

3. Dr. Fatma Outay

Dr. Fatma OUTAY is a senior researcher in Computer Science and Wireless Mobile Networks and Telecommunications. She holds a MS degree in Networks and Telecommunications from The National Engineering School of Tunis El Manar. Dr. fatma received her Ph.D. in Wireless Mobile Networks and Telecommunications from the University of Paris Sud 11, Orsay, France. During her Ph.D and Post Doc at Telecoms Sud Paris, France, Dr. Fatma has participated in several national and international research projects in Wireless and Mobile Networks, in collaboration with Alcatel Lucent, Thales, Orange Labs and other academic institutions in Europe. Prior to her current position at Zayed University, UAE, as an Assistant Professor, Dr. Fatma has joined Bouygues Telecoms in 2012, which is one of the three main Telecoms Operators/ISPs in France, as a “Wi-Fi Expert/Architect” for three years enabling negotiation of SLA agreements and defining technical support and incident management processes with different contributors and suppliers implementing internal and external processes as per ITIL recommendations

4. Prof. Dr. Ansar Yasar

Dr. Ansar-Ul-Haque Yasar received his BS degree in Software Engineering in 2001 from Foundation University Islamabad, Pakistan, MS degree in Computer Science & Engineering in 2007 from Linkoping University, Sweden and Ph.D. in Engineering in 2011 from Katholieke Universiteit Leuven, Belgium. After finishing his Ph.D., he became a senior researcher and a professor at the Transportation Research Institute (IMOB), Hasselt University, Belgium. Furthermore, he has been involved in organization of many international peer-reviewed conferences, summer schools and other scientific events. Dr. Yasar is also a Technical Expert to evaluate project proposals submitted to the European R&D – EUREKA & COST frameworks.

5. Dr. Saleem Iqbal

Dr. Saleem Iqbal Ph.D. received both his BS and MS in Computer Science from the COMSATS, Pakistan and PhD from PERG Lab, Faculty of Computing, UTM, Malaysia in 2015. He is Assistant Professor at University Institute of Information Technology, PMAS-Arid Agriculture University Rawalpindi. Previously, he was with the Department of Computing Science, COMSATS as Lecturer from 2003 to 2007. Saleem worked for four years in Pakistan Federal Government for deployment of ICT projects. His research interests include medium access control and network layer for heterogeneous wireless networks. To his credit, there are 20 publications.

Authors Photographs

Raja Waseem Anwar	
Dr. Anazida Zainal	
Dr. Fatma Outay	
Prof. Dr. Ansar Yasar	
Dr. Saleem Iqbal	

Manuscript Title:

BTEM: BELIEF BASED TRUST EVALUVATION MECHANISM FOR WIRELESS SENSOR NETWORKS

Highlights:

1. The use of Bayesian belief based malicious node detection and isolation mechanism for WSNs.
2. Adopting proposed trust mechanism under varying number of malicious nodes and attacks.
3. Evaluation and validation of the effectiveness of the proposed mechanism.