TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network

Amol R. Dhakne[1] and Prashant N. Chatur[2]

Dept. of CSE, Government College of Engineering, Amravati, India[1,2]

Summary
In wireless sensor network, traditional security mechanisms such as cryptographic methods need a large consumption of resources such as memory, speed, and communication bandwidth. And by using such techniques it is not possible to detect malicious, faulty and selfish nodes that harm to network. Alternatively, trust methods calculate trust of sensor nodes and thereby help to detect malicious, selfish and faulty nodes in Wireless Sensor Network. In this paper, a Trust Calculation based on nodes properties and recommendations (TCNCR) is proposed to calculate trust for wireless sensor network. The proposed technique is very efficient to detect malicious and selfish nodes in wireless sensor network and also allows trusted routing by eliminating malicious nodes. Results of this paper shows that detection rate of our TCNPR method is higher than any other trust model in wireless sensor network. Additionally this paper focuses on different applications where trust methodologies can be used in wireless sensor network.

Key words
Wireless Sensor Network; Trust; Direct Trust; Indirect Trust; Blackhole; Intrusion Detection

1. Introduction

Wireless Sensor Network (WSN) is composed of various sensor nodes that cooperatively monitor environmental conditions such as temperature, pressure, pollutants or motions, etc. Sensor node in wireless sensor network has the ability to sense or read the information from environment and transfer this information to base station. Wireless Sensor network have a various applications in field of battlefield surveillance, health monitoring, etc. Sensor nodes are limited by resources such as memory, power and energy. There are various challenges in the design of wireless sensor network due to wireless environment and unreliable communication. Most critical issue is that these nodes can be compromised and they can perform malicious activities such as dropping of packets, modifications of packet to disturb the normal operations of wireless sensor network. In this paper, Trust Calculation based on Nodes Properties and recommendations method is described for Intrusion detection in Wireless Sensor Network. Intrusion or security attack [1] is any unwanted behaviour in network that can harm the performance of network.

2. Trust Concept

Trust in wireless sensor network can be defined in various ways. According to [2] trust is the degree of reliability about other node for performing certain action by keeping track of all past transaction or interactions with nodes by direct or indirect observation. Trust can also be defined as the level of confidence that one node about other node to get assigned work done within some time. This level of confidence is calculated by one node about other node based on past interaction or transaction history. This trust value depends on time and it can decrease or increase according to evidences available from direct observations or recommendations from trusted neighbouring nodes. To calculate the trust we need some evaluation technique based on some mathematical model. Trust management in wireless sensor network is essential as these can be used in taking decisions about different activities of network [3]. As wireless sensor networks are being used for various applications, these have different needs of security. Working principle of WSN totally depends on cooperativeness and trusting nature of sensor nodes. That is why establishment of trust between sensor nodes is essential one. There are various applications of establishing trust in wireless sensor network. These are described in following section.

3. Applications of Trust in Wireless Sensor Network

In wireless sensor network, there are hundreds of sensor nodes that detect different events from environment continuously or based on occurrence of any event that gives the signal to detection process. The data that is collected can be processed by local sensor node or it can be sent to sink node or base station for processing. So this makes security of wireless sensor network more

Manuscript received December 5, 2016
Manuscript revised December 20, 2016

challenging. While monitoring environmental events, these sensor nodes can be captured by adversary and these can manipulate the sensor nodes. Trust can be used in communication process for data aggregation where amount of transmitted data is reduced while transmission of a data from one node to another node. Sensor nodes can cooperate each other to defend or prevent form malicious attacks or they can work in alternative fashion so as to improve energy and make wireless sensor network to work for long time. Thus, adversary can attack routing protocols, data aggregation or sleeping scheduling of nodes. Also, information about location of sensor nodes is important for some routing protocols such as geographical routing. Therefore by considering above aspects we discuss the different application so trust models in WSNs such as malicious attack detection, secure node selection secure routing, secure data aggregation and secure localization.

3.1 Malicious Node Detection

As sensor nodes in wireless sensor network are deployed in hostile environment, these individual nodes are always prone to be attacked by adversaries due to limited constraints such as limited battery, less computation power and low memory space. It is very important to detect such adversaries in wireless sensor network so as to avoid false information from attackers through compromised nodes. These malicious noes can inject some packets to start different types of attacks such as black-hole attack, selective forwarding attack, or they can implement Denial of Service (DoS) attacks.

So as to overcome the selective forwarding attack a scheme called secure data transmission Scheme (SDTS) is proposed to forward packets in safe manner. In this, first the trust value of every node is calculated to so as to obtain secure route for forwarding the message. And then technique of watermark is applied to detect suspected nodes which are in position to launch selective forwarding attack. In this method initially trust value of each sensor node is set to tvi. Whenever malicious node is detected, trust value of that node is reduced by half of tvi and it becomes (tvi=tvi-1/2tvi). But most of time trust value is decreased due to environmental conditions so it need to be increased by some factor k which is environmental parameter which can be adjusted dynamically in different conditions and new trust value can become tvi = tvi + k. So, if node is considered malicious by doubt, it can again be used later by considering environmental conditions that can affect trust value of sensor node.

Apart from selective forwarding attack, to avoid selfish nodes in wireless sensor networks, in [4] a Data-Centric Dempster-Shafer theory- based Selfishness Thwarting via Trust evaluation (D2S2T2) is proposed. This method based on calculation of trust not only detects selfish nodes but also control effect of false recommendations so as to make network more robust against adversaries.

In [5], a Distributed Trust based Intrusion detection approach have been proposed in wireless sensor network to detect the intrusion based on calculation of trust of sensor node. In this approach, a trust is established based on different factor of sensor node such as honesty, energy, intimacy etc.

3.2 Secure Routing Protocols

In wireless sensor network, it is important that packets need to be routed to destination in secured way. But there are various attacks that harm to WSN routing protocols. Traditional routing protocols such as Geographic Routing (GR) could not prevent or defend against such attacks. That is why secure routing is important in wireless sensor network. There are various secure routing protocols that are proposed by considering the trust factor of sensor nodes. Following table compares different secure routing protocols with respect to methodology, trust calculation, advantages, disadvantages and complexity of particular trust mechanism.

In [6], a trust evaluation scheme is described for resilient geographic routing [T-RGR] for wireless sensor network.in this trust algorithm works in distributed fashion so that each node is able to monitor the behaviour of one-hop neighbour node. If neighbour node forwards the packet successfully, source node increases the trust value of neighbour node with some predefined size at every step. Otherwise it decreases the trust value by some steps size. But this algorithm is considered to be costlier because of scarcity of resources .

In [7], Efficient Monitoring Procedure in a Reputation system is implemented which consist of three major components for monitoring, rating and response generation. In this nodes that are in ON state perform the monitoring. Rating calculates risk of observing node to perform routing function. Risk value is one that describes nodes previous behaviour of unsuccessful routing. In response component risk values computed by rating component are analysed with respect to distance and energy to choose the best next hop for operation of routing.

In [8], Efficient Reputation- based Routing Mechanism [ERPM] is proposed. In this mechanism author added some mobile nodes in WSN. In this when node A collects required number of reputation values of node B, it starts aggregating information. Firstly, median is calculated from reputation values and then reputations that are below threshold from median are discarded. Reputations that have been left are weighted before average reputation. Weighted reputation is calculated by using following formula:

$$RW_{C\rightarrow B} = TN_{A\rightarrow C} \times R_{C\rightarrow B} \times AG_{C\rightarrow B} \qquad (1)$$

Where, $TN_{A\rightarrow C}$ is the trust that node A granted to node C, $R_{C\rightarrow B}$ is the reputation value that node C granted to node B and which is transmitted to node A. $AG_{C\rightarrow B}$ is of reputation information $R_{C\rightarrow B}$ which is collected by node A.

After calculating the all reputation contribution, final weighted average of all reputation for node B is calculated as follows:

$$TN_{A\rightarrow B} = \frac{\sum_{C\in Contributor} RW_{C\rightarrow B}}{\sum_{C\in Contributor}(TN_{A\rightarrow C} \times AG_{C\rightarrow B})} \qquad (2)$$

This mechanism has succeeded to maintain very high success rate. In this, success rate is calculated based on number of packets sent by normal nodes that are received by BS in same sequence and are not corrupted by malicious node.

In [9], a routing protocol that is based on the trust factor is presented and is called as Trust-Aware dynamic Routing Framework (TARF). TARF consist of different components such as Trust Metrics Model, Behaviour detection, Trust Calculation Model and Trust-Aware Routing model. In trust metric model different performance metrics are defined such as packet modification observation, packet forwarding observation and routing verification. These are used to detect the misbehaviour in next phase of behaviour detection. Output from behaviour detection model is used to compute the trustworthiness by Trust evaluation model. Trustworthiness T is calculated directly based on reputation R_{E} and risk value R_{I} as follows:

$$T = \begin{cases} (1-\alpha,\alpha) \times (R_E, R_I)^T, & 0 < \alpha < 1 \\ R_I, & if\ \alpha = 1 \\ R_E, & if\ \alpha = 0 \end{cases} \qquad (3)$$

When deciding a route most direct policy can be considered which selects the next hop having largest trustworthiness value. However, this can result in large delay. That is why, author proposes a trust-aware routing criterion to integrate trust model with routing protocols that avoid introducing large delays. Routing Criteria (RC) is defined in following manner:

$$RC = \frac{C}{T} \quad \text{or} \quad RC = C \times T \qquad (4)$$

Here C is original routing criterion value for sensor node to make a decision about routing. T is called as trustworthiness value of sensor node. If C is represented by criteria's such as delay, hop count, cost etc. then first formula is applied, if C is represented by criteria such as bandwidth etc., then second formula is considered. From above formulas we can say that minimum the value of RC, minimum will be delay and maximum will be the trustworthiness. With some modifications TARF can be applied to different routing protocols.

In [10], a model based on trust is proposed called as Trust-based Cross Layer Model (TCLM), that guarantee trusted route from source to sink node while isolating malicious nodes. Value of Trust t and treatment ration r are computed based on statistics of packets for every neighbour node. Here trust value reflects the degree of belief which is dependent on reliability neighbour node to deliver a packet. Treatment ratio is used to calculate the statistical confidence in belief. Suppose if L is number of packets correctly forwarded by sensor node and N is total number of packets forwarded, then trust (t) and treatment ratio (r) can be calculated as follows:

$$t = \frac{L}{N}, \qquad r = 1 - \frac{\sqrt{12L(N-L)}}{(N+1)N^2} \qquad (5)$$

All the trust based routing methods are described in table with respect to methodology, trust values, advantages, performance limitations and complexity in Table 1.

3.3 Secure Data Aggregation

Data aggregation is the process in which data is gathered from different sensor nodes and then these are expressed in some summary before sending it to base station or sink node. Data aggregation is helpful to minimize the number of transactions. To improve energy efficiency and network lifetime, data aggregation is very important in wireless sensor networks. Large amount of energy can be saved when sensor nodes are far away from base station. But as sensor nodes can be deployed in hostile environment, attackers can inject wrong information or forge values of aggregation without getting detected. That is why, security is important issue in data aggregation for Wireless Sensor Networks.

Sensor nodes in WSN can perform different activities such as sensing, aggregating data or forwarding data. In [11], a Social Estrangement Trust Management model [SETM] is proposed for secure data aggregation. In this model, sensor node senses data from environment and forwards it to forwarder or aggregator, a forwarder forwards data again to aggregator or base station. In this model three types of trust such as forwarding trust, sensing trust and aggregation trust are considered. This model works well against attacks such as selective forwarding attack. Disadvantage of this model is that it cannot predict about future behaviours. If node behaved well in past, it is said to be reliable.

Table 1: Comparison of trust based secure routing protocols

Trust Mechanism	Method	Trust Values	Advantages	Disadvantages	Complexity
T-RGR [6]	Not considering exact trust Mechanism	[0,1]	Considered to avoid Sybil, selective forwarding and black hole attacks	Does not work against collaborative attacks	Need a lot of memory and space to handle packet forwarding
EMPIRE [7]	Not considering exact trust Mechanism		Reduces activities to monitor each node	Only described to avoid non-forwarding attack	Complex to manage between On-OFF state
ERPM [8]	Weighting	Trust calculated based on neighbor nodes recommendations	Prevent from effects of hostile nodes	Need a lot of energy to select best possible route	Complexity is Less
TARF [9]	Matrix Theory	Calculates reputation and risk	Good against Selective forwarding, black hole and message modification attacks	Unable to characterise misbehaviour in routing based on trust metrics	Need a lot of energy and memory to monitor behaviour of neighbour nodes.
TCLM [10]	Beta distribution and Bayesian statistics	[0,1], calculation of treatment ratio and trust	Work very well even if number of malicious nodes is high	Scales only to highly dense WSNs	Watchdog hardware needed to view data sent and received between nodes.

3.4 Secure Localization

Localization plays very important role in various applications of wireless sensor network. It is very important for users to get correct information about location so as to accomplish functioning of related application. Idea behind the localization is that deployed nodes with known co-ordinates (GPS enabled nodes) transmit some information about their co-ordinates to other nodes so that other nodes can localize themselves. In this idea, deployed node is called as anchor node and transmitted information is called as beacon. So, here it is important to identify the malicious anchor nodes so as to avoid false information about actual location.

In [12], Distributed Reputation based Beacon Trust System (DRBTS) is proposed. This is the first concept of reputation to exclude malicious anchor nodes. In DRBTS, every anchor node keeps record of one hop misbehaving anchor nodes and updates reputation values of corresponding anchor nodes in Neighbour-Reputation-Table (NRT). In this model whenever any sensor node want to know information about location, all neighbour anchor nodes transmit their location information to requesting node. It can then decide location using locations of neighbour anchor nodes and by comparing it with true locations. If difference is less than certain margin, it is considered as benign and its reputation value is increased. If difference is large than certain margin, corresponding anchor node is considered malicious and its reputation value is decreased.

Finally majority voting scheme can be used by sensor node to decide whether to use or not to use given beacon information about location obtained through NRT. Sensor nodes are supposed to get votes for trustworthiness at least from half neighbours in order to trust beacon information of nodes. Even though DRBTS can reduce effect of malicious node up to certain limit, it cannot resist the conspiracy type of attacks. Another disadvantage of this model is that reputation information of nodes is updated by themselves. If anchor node itself gets compromised, they can disturb the reputation values and cannot update values of reputation in normal way. Therefore, this model is always vulnerable to malicious anchor nodes. Also, DRBTS does not mention any details about how the reputation values of anchor node are calculated.

In [13], Trust based secure localization scheme (TBSL) is proposed where reputation of anchor node is calculated based on anchor node’s identity and behaviour. Thus, TBSL is more effective than DRBTS in terms of fighting against attacks that are originated from compromised anchor nodes. Another difference of TBSL from DRBTS is that every unknown node calculates the average value of trust collected from neighbour anchor nodes after calculation of trust values of anchor nodes. After that, every unknown node estimates its own position based on selected trustworthy anchor nodes whose trust values are above threshold value. Here unknown node estimates position through maximum likelihood estimation. Compared to DRBTS, TBSL is more simple and energy efficient for Wireless sensor network.

3.5 Secure Node Selection

In WSNs, there is cooperation among sensor nodes to accomplish particular task such as tracking or localization. Sometimes, malicious nodes take benefit of cooperativeness of sensor nodes to attack whole network. For proper cooperation, appropriate nodes need to be selected and nodes that do not have ability to complete the task need to be excluded. Therefore, in [14, 15] , a Reliable Sensor Selection algorithm with power aware Trust management is proposed.

In this model every senor node is described by Node (ID,A,V,T), where ID is identity of node, A is set of Attribute of node ID, V is values of attributes of node and T is the trust values of attributes of node ID . Trust value for attribute Ai can be calculated by $Ai = \frac{Si}{Ci}$, where Si indicated number of successful cooperation and Ci is the number of cooperation among neighbour nodes. In this algorithm three trust values are calculated such as Direct Trust, Indirect Trust and Integrated trust.

Direct Trust values are calculated by using following equation:

$$T_{direct} = \frac{\prod_{i=1}^{n} TAi}{\prod_{i=1}^{n} TAi + \prod_{i=1}^{n}(1-TAi)} \qquad (6)$$

Indirect Trust values are calculated by:

$$T_{indirect} = W_{reliable} \times T_{reliable} + W_{strange} \times T_{strange} \qquad (7)$$

Where, $T_{reliable}$ indicate trust value which is returned by reliable third party nodes, $T_{strange}$ indicate trust value which is returned by strange third party nodes, $W_{reliable}$ indicate weight value of reliable third party node, $W_{strange}$ indicate weight value of strange third party node and $W_{reliable} + W_{strange} = 1$. And at last, integrated trust value is calculated by summing weighted trust values of direct trust and indirect trust.

4. Technique for Trust Calculation

In this section, Trust Calculation based on nodes properties and recommendations from neighbours [TCNPR] method is proposed to evaluate trust value of sensor node to detect intrusions in WSN. Based on this method any node of WSN can calculate trust of neighbour nodes. Neighbour nodes are those that belong to radio range of sensor node. Trust is the level of confidence that depends on time. Trust value may change with respect to time based on nodes behaviour while performing transactions among them. Trust can be calculated based on past experience with node and the recommendations that are given by neighbour nodes. Here past experience means behaviour of node based on different factors i.e. we call them as trust metrics [16][17]. Trust calculated based on trust metrics is called as Direct Trust (DT). Trust calculated based on indirect information obtained by recommendation through neighbour node is called as Indirect Trust (IT). Overall Trust (OT) is calculated based on direct and indirect trust based on individual impact of type of trust. In Fig. 1. Node A is evaluating the trust of node B. It calculates the direct trust based on direct experience information and indirect trust is calculated based on information which is given by neighbour nodes.

There are various metrics to calculate the trust of sensor node [17] which are given in following table:

Table 2. Metrics for Trust Calculation

Battery lifetime/Energy
Packet Delay
Data packets forwarded
Reputation
Sensing Communication
Reputation Packet Precision/Integrity
Honesty
Intimacy
Unselfishness

Every sensor node in WSN is expected to update the values of trust metric about its neighbour node for every activity occurring in network. The record created by observation of neighbour nodes is used to calculate the Direct Trust (DT) of neighbour node. Indirect trust (ID) of any neighbour node can be calculated based on information got from all other neighbour nodes.

Some of the trust metrics are defined as follows:

Packet Forwarding: this metric is used to detect the denial to forward any packet which has been sent from source node to neighbour node for further forwarding.

Availability to hello message: detection of nodes that are within radio range and are able to forward the packets.

Packet Delay: it is the metric which detects delay in time packet carries to reach to destination node successfully.

Packet Integrity/Precision: checking that no change has been made in packet while transmission from source to destination.

Remaining Energy: although energy is not pure metric of trust, considering energy contributes to balancing of node.

Reputation: In trust calculation technique neighbour nodes can be requested to provide indirect information about node. This will be helpful whenever there is no direct information available about trust of node.

In this trust calculation method we divide trust metrics into two types such as high priority metrics and low priority metrics. High priority trust metrics are helpful to see the main functionality of a node. That is why, these trust metrics are not supposed to go below the level of trust threshold level. For example, values of trust metrics such as data packets forwarded, control packet forwarded are not supposed to be less than the higher priority threshold as functionality of nodes are hidden within these metrics. Other metrics of trust can be considered as low priority category of trust metric.

Direct trust of any neighbour node can be calculated based on the higher trust metric and lower trust metric values. Higher priority Trust metrics values are either multiplied or their Geometric mean value is considered as nodes are supposed to maintain the minimum trust threshold of high priority trust metric. Same to this, Lower Priority Trust metrics either averaged or their arithmetic mean value is considered. To calculate the direct trust value, these two categories of trust metrics are combined by applying some weight to each type. Here node can become malicious either when value of higher trust metric is falling down the threshold value or when overall value of direct trust is going below the threshold value for direct trust

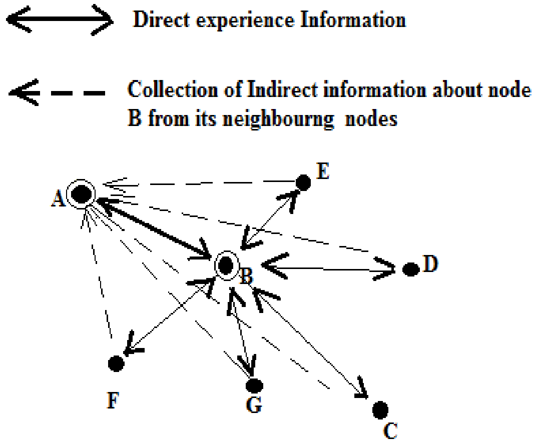

Direct experience Information
Collection of Indirect information about node B from its neighbourng nodes
A
B
C
D
E
F
G

Fig. 1 Node A evaluates trust on node B

Indirect trust of any node can be calculated based on recommendations from neighbour nodes. Neighbour nodes can be differentiated into most trusted neighbour or normal neighbour. Every node maintains history of trust apart from trust metric data. Based on the history, some nodes are considered highly trusted and other nodes are considered as less trusted. High trusted neighbour nodes are considered for recommendation as they can recommend positively. Recommendations of low priority nodes are averaged. To calculate the indirect trust these two trusts are weighted and then combined. Here node is considered malicious either when most trusted neighbour is not recommending or when overall indirect trust value is below the indirect trust threshold value.

Finally overall trust sometimes called as total trust T can be computed by combining the direct trust (DT) and Indirect trust (IT). Our methodology combines these two to obtain Total Trust (T).

4.1 Direct trust (DT)

For any trust calculation based model it is important to collect the data for trust calculation. Different trust metrics can be used to determine the direct trust of neighbour node. Different trust metrics that can be considered are given in [17]. These trust metrics can be helpful for decision making about a node. All trust metric s can have minimum trust threshold for different applications or for different group of trust metrics. Our trust calculation mechanism strictly consider that node is trusted only if value of given trust metric is above minimum trust threshold otherwise it is considered as not trusted. This is the major advantage of trust model compared to other. This model helps to identify intrusions and differentiates among normal node and malicious nodes while routing in WSN.

Trust metrics are categories into two types called as high priority and low priority as shown in Fig. 2. Suppose that $tm_k^{P,Q}$ is set of different high priority trust metric of node P on node Q for different trust metrics where k= 1 to m. similarly, suppose that $tm_r^{p,q}$ is set of different low priority trust metric of node P on node Q for different trust metrics where r= 1 to n .

In our trust calculation model , direct trust of any neighbour node is calculated based on weighted sum of geometric mean of high priority trust metric and arithmetic mean of low priority trust metric. Here value of each high priority trust metric is larger than threshold value. Direct Trust (DT) of neighbour node can be calculated based on following equation.

$$DT^{P,Q} = W_H^{DT} \times \Pi \ [(tm_1^{P,Q} , tm_2^{P,Q} , tm_3^{P,Q} , \ldots, tm_m^{P,Q})]^{(1/m)} + W_L^{DT} \times \frac{1}{n} [\Sigma (tm_1^{p,q} , tm_2^{p,q} , tm_3^{p,q} ,\ldots, tm_n^{p,q})]$$

$$DT^{P,Q} = W_H^{DT} \times [\prod_{k=1 \ to \ m} tm_k^{P,Q}]^{1/m} + W_H^{DT} \times \frac{1}{n} [\sum_{r=1 \ to \ n} tm_r^{p,q}] \qquad (8)$$

In above equation W_H^{DT}, W_L^{DT} are the weights assigned to high priority and low priority trust metrics respectively such that $W_H^{DT} + W_L^{DT} = 1$.

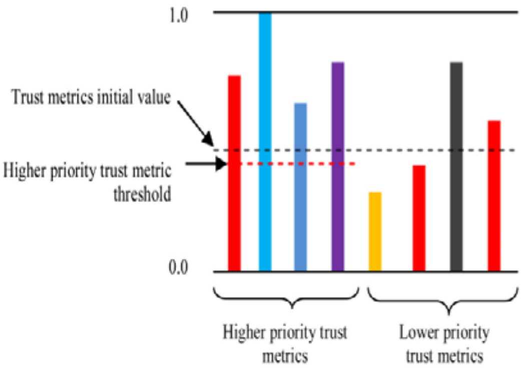


Fig. 2 Different levels of different trust metrics

4.2 Indirect Trust (IT)

Indirect trust of any neighbour node can be calculated based on the indirect information obtained through other neighbour nodes. Here neighbour nodes can be classified in two types based on trust of neighbour node such as most trusted and low trusted/ normal neighbour nodes. Geometric mean is calculated for most trusted nodes and arithmetic mean is calculated for low trusted nodes while calculation of indirect trust of particular sensor node. Consider that some set of are located in network topology as shown in Fig. 3.
They are P, Q, C, D, E, F, G and I. We are going to calculate the indirect trust of node P on node Q i.e. $IT^{P,Q}$. Here node P collects the recommendation from all other neighbour nodes about node Q. In this example C, D, E, F, G and I are neighbours. Suppose that the recommendations that have been collected are $T^{C,Q}$, $T^{D,Q}$, $T^{E,Q}$, $T^{F,Q}$, $T^{G,Q}$, $T^{H,Q}$ and $T^{I,Q}$. Out of all these nodes suppose that node G and F are most trusted neighbours of P. Indirect trust is combination of indirect information obtained through nodes that have high priority and normal neighbour nodes. Geometric mean will be applied to high priority nodes and arithmetic mean will be applied to less priority nodes. W_H^{IT} and W_L^{IT} are the weights assigned to high priority and low priority nodes respectively. According to figure 3, following equation can be used to calculate the indirect trust in general

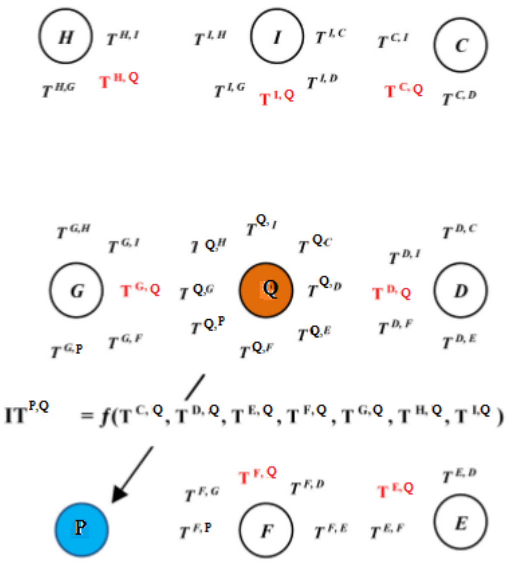


Fig. 3 Indirect trust of node P on node Q

IT= Geometric mean of high priority neighbour nodes + Arithmetic mean of Low priority neighbour nodes
Indirect trust of node P on Q can be computed by using following equation.

$$IT^{P,Q} = W_H^{IT} \times [\prod_{i=1 \, to \, t} W_{P,Ni} \times T^{Ni,B}]^{1/t} + W_L^{IT} \times \frac{1}{s} \sum_{j=1}^{s} (W_{P,Nj} \times T^{Nj,Q})$$

(9)

Where $W_{P,Nj}$ is recommendation weight made by jth neighbour of node P.

4.3 Trust

Total trust or Overall trust T of any neighbour node can be calculated based on weighted summation of direct trust DT and indirect trust IT.

$$T = W_D \times DT + W_I \times IT$$

Here W_D is the weight associated with direct trust and W_I is the weight associated with indirect trust such that $W_D + W_I = 1$. Total trust between sensor node P and Q can be evaluated as follows.

$$T^{P,Q} = W_D \times DT^{P,Q} + W_I \times IT^{P,Q}$$

$$\begin{aligned} T^{P,Q} = W_D \times \{ & W_H^{DT} \times [\prod_{k=1 \, to \, m} tm_k^{P,Q}]^{1/m} + \\ & W_H^{DT} \times \frac{1}{n} [\sum_{r=1 \, to \, n} tm_r^{p,q}] \} + \\ & W_I \times \{ W_H^{IT} \times [\prod_{i=1 \, to \, t} W_{P,Ni} \times T^{Ni,B}]^{1/t} + \\ & W_L^{IT} \times \frac{1}{s} \sum_{j=1}^{s} (W_{P,Nj} \times T^{Nj,Q}) \} \end{aligned} \qquad (10)$$

Where P is sensor node that calculated its trustworthiness on node Q,
m is metric having high priority,
n is metric having low priority
t is most trustful neighbour, s is any ordinary neighbour
$tm_k^{P,Q}$ is the kth higher priority trust metric of node P on node Q
$tm_r^{p,q}$ is the r th lower priority trust metric of node P on node Q
W_H^{DT} is the weight for higher priority trust metric,
W_L^{DT} is the weight for lower priority trust metric
W_H^{IT} is the weight for higher priority neighbour
W_L^{IT} is the weight for lower priority neighbour
$W_{P,Nj}$ is recommendation weight made by jth neighbour of node P
$T^{Nj,Q}$ is the trust obtained from neighbour N_j about node Q
W_D is weight for direct trust and W_I is weight for indirect trust.

4.4. Algorithm for Trustworthy Node Selection for Transmission of Packet

This algorithm selects neighbour node for transmission of packet in trustworthy manner. This algorithm first find out the neighbour nodes that are trustworthy based on trust metric data. If trust value of node is greater or equal to threshold of trust then it is selected for transmission of packet. But if it does not found any trustworthy neighbour node then it communicates with neighbour nodes and obtain indirect information from all neighbours within its radio range. Then it calculates the trust and selects best node. If trustworthy node is found in initial step, a lot of energy will be saved. If no trustworthy node is found within radio range then it increases the radio range of communication to search trustworthy neighbour nodes through indirect information. This will consume some energy. Like this this calculation method is helpful to save energy of node till the trust of neighbour node is larger than or equal to trust threshold. This helps to save battery power of node and increases the lifetime of whole WSN. Thus this adaptive TCNPR is not just energy efficient but it also minimizes communication overhead as explained in Algorithm 1.

Algorithm 1: Algorithm for trustworthy node selection for transmission of packet

```
While (packet is ready) {
    Calculate trust of all neighbour nodes;
    for all neighbour nodes ($n_i$) {
        If (Trust of node $n_i \geq T_{th}$ ){
            forward packet to neighbour node $n_i$;
            trustworthy_node_found = ‘yes’ ; return; }
        trustworthy_node_found = ‘no’;}
    If (trustworthy_node_found = ‘no’) { // perform node energy consumption operation
            Obtain indirect information form neighbour nodes;
            Calculate trusts of all neighbour nodes;
            for all neighbour nodes ($n_i$) {
                If (Trust of node $n_i \geq T_{th}$) {
                    forward packet to neighbour node $n_i$;
                    trustworthy_node_found = ‘yes’ ; return;}
            trustworthy_node_found = ‘no’; }}
    If (trustworthy_node_found = ‘no’) {// perform maximum node energy consumption operation
            Increase radio range of node r;
            Obtain indirect information form neighbour nodes;
            Calculate trusts of all neighbour nodes;
            for all neighbour nodes ($n_i$) {
                    If (Trust of node $N_i \geq T_{th}$) {
                        forward packet to neighbour node $n_i$;
                        trustworthy_node_found = ‘yes’ ; return; }
                    trustworthy_node_found = ‘no’;}}
    If (trustworthy_node_found = ‘no’)  {// perform maximum node energy consumption operation
        Forward packet to neighbour having highest trust value;
        Return;} } //endwhile
```

4.5 Advantages

This method has a lot of advantages than existing methods. This method allows calculating trust of all neighbour nodes even if trust threshold is not decided. This method can distinguish between normal node and malicious node even before selection of neighbour node for transmission of packet. According to the application requirement, this method allows us to assign more weights to different trust metric, neighbour nodes. Methods direct trust and indirect trust calculation is not based on calculation of average of different trust metric like in other trust models. If calculation would have been average of different trust metric then sometimes node could have been considered trustworthy, even if its major trust metrics like data packets forwarded, control packets forwarded are going below T_{th}. Such kind of situation can arose in Sybil attack. In our method, even if single trust metric fails to form trust, node can be considered as malicious. So in this trust calculation method, it is easy to detect malicious nodes and discard them from transaction with normal nodes.

5. Simulation Result

Intrusions can be detected by this trust calculation based on nodes properties and recommendation (TCNPR) method which run on sink node. Performance of our method has been evaluated in ns2. We have evaluated the performance of our trust calculation mechanism TCNPR with routing protocol. The simulation setup settings and other assumptions are as follows:

Table 3 : Simulation Setup parameters

Simulator	Network Simulator 2
Simulation Of Nodes	50
Interface Type	Phy/Wirelessphy
Channel	Wireless Channel
Mac Type	Mac/802_11
Queue Type	Queue/Droptail/Priqueue
Queue Length	201 Packets
Antenna Type	Omni Antenna
Propagation Type	Two ray Ground
Size Of Packet	Five Hundred And Twelve

Traffic	Tcp

We have compared our method TCNPR with An Efficient Distributed Trust model in Wireless sensor network [16] for selective forwarding and black hole attack. Fig. 4 shows that the detection rate of our TCNPR is higher than EDTM for Selective forwarding attack. Fig. 5 shows that detection rate of our TCNPR is higher than EDTM for Blackhole attack. Thus our Trust Calculation based on nodes properties and recommendations [TCNPR] method is more efficient than any other trust model in wireless sensor network.

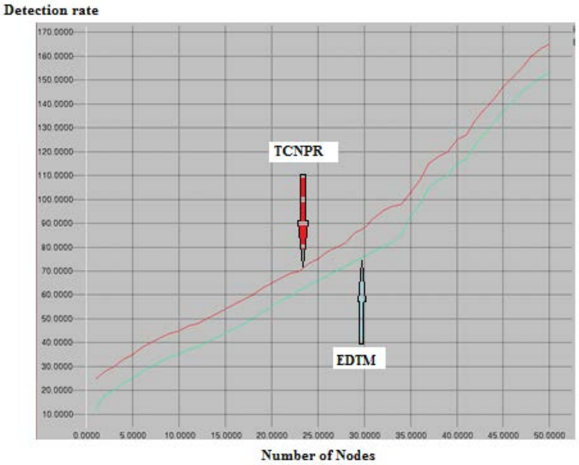


Fig. 4 Detection rate for Selective Forwarding attack

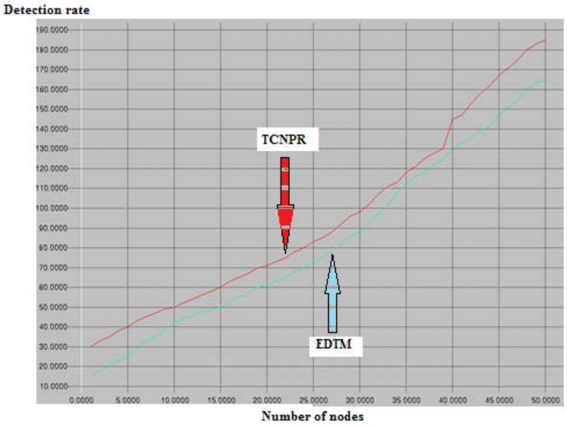


Fig. 5 Detection rate for Blackhole attack

6. Conclusion

TCNPR trust calculation method is able to detect malicious nodes in wireless sensor network and provide trustworthiness between sensor nodes and their neighbours based on different trust metric and recommendations from neighbour nodes. Direct trust is calculated based on properties of nodes which are judged by different trust metrics and indirect trust is calculated based on recommendations from neighbours. We discussed that some properties of node can be of higher priority and other can be of lower priority. Also priority of trust metrics changes according to the application type. We have shown how detection rate of our TCNPR is more than other trust methodology. Our algorithm shows how adaptive energy consumption operation helps to increase radio range of sensor node to handle situation when no any trustworthy node is available for packet transfer. This method not only just detects malicious attacks but also tries to minimize communication overhead efficiently.

Acknowledgments

Authors are grateful to the Technical Education Quality Improvement Program (TEQIP- II) unit at Government College of Engineering, Amravati for providing research facilities and funding.

References

[1] A. R. Dhakne, P. N. Chatur, 2016. Detailed Survey on Attacks in Wireless Sensor Network. Proceedings of the International Conference on Data Engineering and Communication Technology,Vol. 469 of the series Advances in Intelligent Systems and Computing , Springer, pp 319-331. https://dx.doi.org/10.1007/978-981-10-1678-3_31

[2] Momani, M., (2008). Bayesian Methods for Modelling and Management of Trust in Wireless Sensor Networks. Ph.D. Thesis, University of Technology, Sydney.

[3] Lopez, J., Roman, R., Agudo, I. and Fernandez-Gago, C. (2010) Trust Management Systems for Wireless Sensor Networks: Best Practices. Computer Communications, 33, 1086-1093. http://dx.doi.org/10.1016/j.comcom.2010.02.006

[4] J. Konorski, R. Orlikowski, 2009. Data-centric Dempster–Shafer theory-based selfishness thwarting via trust evaluation in MANETs and WSNs. In Proceedings of the 3rd International Conference on New Technologies, Mobility and Security, pp. 74–78.

[5] A. R. Dhakne and P. N. Chatur, 2015. Distributed Trust based Intrusion Detection approach in wireless sensor network. *2015 Communication, Control and Intelligent Systems (CCIS)*, IEEE, Mathura, pp. 96-101. DOI: 10.1109/CCIntelS.2015.7437886

[6] K. Liu, N. Abu-Ghazaleh, K.D. Kang,2007. Location verification and trust management for resilient geographic routing, Journal of Parallel and Distributed Computing 67 (2). pp 215–228.

[7] I. Maarouf, U. Baroudi, A.R. Naseer,2009. Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks. IET Communications 3 (5) . pp 846–858.

[8] N. Lewis, N. Foukia, 2008. An efficient reputation-based routing mechanism for wireless sensor networks: Testing the

impact of mobility and hostile nodes, in: Sixth Annual Conference on Privacy, Security and Trust, pp. 151–155.

[9] H. Deng, Y. Yang, G. Jin, R. Xu, W. Shi, 2010. Building a trust-aware dynamic routing solution for wireless sensor networks. In IEEE Globecom 2010 Workshop on Heterogeneous, Multi-Hop Wireless and Mobile Networks. pp. 153–157.

[10] H.A. Rahhal, I.A. Ali, S. Shaheen,2011. A novel trust-based cross-layer model for wireless sensor networks. 28th National Radio Science Conference, NRSC. pp. 1–10.

[11] N. Poolsappasit, S. Madria,2011. A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network. International Conference on Parallel Processing. pp. 138–147.

[12] A. Srinivasan, J. Teitelbaum, J. Wu,2006. DRBTS: Distributed reputation-based beacon trust system, in: 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. pp. 277–283.

[13] T. Zhang, J. He, Y. Zhang, 2011. Trust based secure localization in wireless sensor networks. 2nd International Symposium on Intelligence Information Processing and Trusted Computing, IPTC. pp. 55–58.

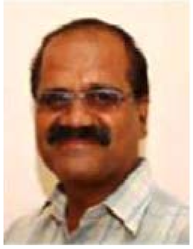
[14] G. Han, D. Choi, T.V. Nguyen, 2007. A reliable sensor selection algorithm for wireless sensor networks. 3rd IEEE/IFIP International Conference in Central Asia on Internet. pp. 1–4.

[15] G. Han, D. Choi, W. Lim, 2007. A novel sensor node selection method based on trust for wireless sensor networks. International Conference on Wireless Communications, Networking and Mobile Computing. pp. 2397–2400.

[16] Zahariadis, T., Leigou, H.C., Trakadas, P. and Voliotis, S. (2010). Mobile Networks: Trust Management in Wireless Sensor Networks. European Transactions on Telecommunications, 21, 386-395.

[17] Trakadas, P., Maniatis, S., Zahariadis, T., Leigou, H.C. and Voliotis, S. (2009) A Novel Flexible Trust Management System for Heterogeneous Sensor Networks. International Symposium on Autonomous Decentralized Systems, ISADS 2009. Athens, 23-25 March 2009, 369-374.

Amol R.Dhakne received B.E. Information Technology in 2010 from Jawaharlal Nehru Engineering College, M.E. Computer Science and Engineering in 2013 from Government College of Engineering both affiliated to Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India. Since from July 2014, he is Ph.D. Research Scholar under TEQIP-II at Government College of Engineering, Amravati affiliated to Sant Gadge Baba Amravati University, Amravati. His research interests include security, trust management, Intrusion detection, network security, wireless sensor network, mobile ad hoc network.



P. N. Chatur has received his M.E. degree in Electronics Engineering from Govt. College of Engineering, Amravati, India and Ph.D. From Amravati University. He has published hundred and ten papers in conferences and journals. His area of research includes Wireless Sensor Network, Artificial Neural Network Data Mining, Data Stream Mining and Cloud computing. Currently he head of Computer Science and Engineering Department at Government College of Engineering Amravati, Maharashtra, India. At present he is engaged with energy efficiency and security in wireless sensor network.