ISSN: 2093-5374 / E-ISSN: 2093-5382

Trust based Routing – A Novel Approach for Data Security in WSN based Data Critical Applications

B. Sreevidya[1*], and Dr.M. Supriya[2]

[1*]Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru,
Amrita Vishwa Vidyapeetham, India. b_sreevidya@blr.amrita.edu,
https://orcid.org/0000-0002-0876-3307

[2]Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru,
Amrita Vishwa Vidyapeetham, India. m_supriya@blr.amrita.edu,
https://orcid.org/0000-0001-6147-7142

Received: September 02, 2023; Revised: November 05, 2023; Accepted: January 07, 2024; Published: March 30, 2024

Abstract

Wireless technology has changed the way entities communicate with one another. Wireless networks have created several opportunities in fields such as military, health care, and habitat monitoring, to name a few. However, only a few data-critical applications are built on wireless sensor networks, such as border reconnaissance, detecting infringement, and patient monitoring. These applications require the processing of a large amount of private data. Because most applications are data-sensitive, securing data transmission among wireless sensor networks is crucial. While incorporating data security, the most important requirement of wireless sensor nodes being energy optimized also need to be kept in consideration. There are various forms of assaults that are relevant in Wireless Sensor Networks (WSN). Attacks like Black Hole attacks, sink hole attacks, False data Injection attacks etc. are the most commonly seen attacks on WSNs. The common element in all these attacks is the concept of malicious / compromised node - a node which either drops / modifies the data content while forwarding it. Existing techniques for data security generally use cryptographic algorithms, but the use of cryptographic algorithms is in contrast with the energy optimization requirement of sensor nodes. An energy efficient data security scheme needs to be developed. The proposed system analyses several attacks and proposes a multi-layer data security approach to prevent change of data / dropping of data by the compromised nodes. The proposed system is a routing protocol referred as Trust Based Routing (TBR). A concept of trust value of a node is the core idea of TBR. Forwarding node is selected based on highest trust value and thus avoid malicious / compromised nodes from being involved in the routing process. The trust factor is calculated by considering the number of packets dropped, packets rejected, and the node's remaining energy. The idea of TBR is enhanced by incorporating the concept of past trust and trust of node towards a specific destination. This proposed scheme is referred as Extended Trust Based Routing (ETBR). This scheme is further enhanced by including Direct Trust, Indirect Trust and Energy Trust concepts. This scheme is referred as Consolidated Trust Estimation – Trust Based Routing (CTE-TBR). Network Simulator NS2 is used to simulate the proposed schemes. Various network factors are compared to classic Adhoc On-Demand Vector (AODV) and newly proposed schemes. The result indicates the effectiveness of the proposed data security scheme in terms of energy efficiency and Packet Delivery ratio (PDR).

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 1 (March), pp. 27-41. DOI: *10.58346/JOWUA.2024.I1.003*

*Corresponding author: Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India.

Keywords: Wireless Sensor Networks, Data Transmission, Security Attacks, Trust based Routing, Direct Trust, Indirect Trust, Energy Optimization.

1 Introduction

Wireless Sensor Networks (WSNs) are largely used in many of the domains like defense, healthcare, logistics, surveillance etc. The main advantage of brining in WSN in such domains is the scalability, mobility and easier data collection & exchange. Wireless Sensor Networks are collection of nodes which are equipped with sensors and actuators which help he nodes to collect data and act up on the environment based on the commands the nodes receive. With the integration of WSN with existing systems, it is possible to remotely monitor the vital body parameters of a patient and provide drug dosages based on the analysis of the parameters measured. This brings revolutionary change to the healthcare sector making it possible for the people from rural remote areas to get access to advanced medical support through WSN based remote healthcare systems. In similar lines, it is possible to remotely monitor hostile environments closer to the border for intrusion as well as surveillance (Ram & Chakraborty 2024).

The critical aspect of the WSN based systems explained previously like border surveillance system or remote patient monitoring system is the security of data being exchanged between the various end points of the system. Wireless Sensor Networks based applications traditionally doesn't give much attention towards data security as the data security schemes are computationally complex and employing such complex systems on WSN will increase the energy consumption due to which the WSN system will ran out of energy faster (Sreenivasu et al., 2022). Even though achieving data security in WSN based applications is a tricky scenario, the WSN based applications getting deployed in healthcare as well as defense domains are data critical applications. Various attacks which aim at data critical applications deployed over WSN exists and majority of them belongs to a category where one or more nodes of the WSN becomes the attacker node. Examples of such attacks are Black-Hole attacks, Grey-Hole attacks, Sink-Hole attacks etc. Majority of researchers pointed to the fact that one among the above-mentioned attack – False Data Injection (FDI) attacks is the most critical and damaging attacks on WSN applications. In FDI attacks, one more node turn out to be malicious nodes which injects / manipulates the data being exchanged between nodes in the WSN application (Kaur & Mahajan 2013).

Traditionally cryptography is suggested as the best solution to data security over networking applications, but the computational complexity of the cryptographic schemes make it difficult to implement them in WSN based applications. An alternate approach to ensure data security is the concept of trust. Trust value of a node is the measure of the node's capability to handle data securely, thus achieving high data security (Costa et al., 2010). Trust value concept is used in various network layers like transport layer, network layer, datalink layer etc. In transport layer, trust value is used to distinguish applications (source / destination) into malicious and non-malicious categories. In network layer, trust value is used in routing process where trust value of forwarding nodes is computed and node with highest trust value is selected for forwarding the data packets. This is referred as Trust Based Routing (TBR) – a routing scheme which used trust value of forwarding nodes to decide on next forwarding node is developed for network layer. The trust computation uses number of packets forwarded & dropped, remaining energy, delay and reputation. Since the trust value changes with respect to time, it is sensible to include past trust also while calculating trust of a node. Also trust of a node is to be interpreted as trust of a node towards a specific node. The Trust Based Routing Scheme is enhanced with the above specified information and the new routing scheme is referred as Extended Trust Based Routing (ETBR). Further enhancement to ETBR included a comprehensive trust estimation process which consider 3 different aspects of trust namely Direct Trust, Indirect Trust and Energy Trust. A weighted average of these different trust factors provides the trust value of a node and this modified scheme is referred as Comprehensive Trust Estimation – Trust Based Routing (CTE-TBR). Fig. 1 illustrate the proposed system.

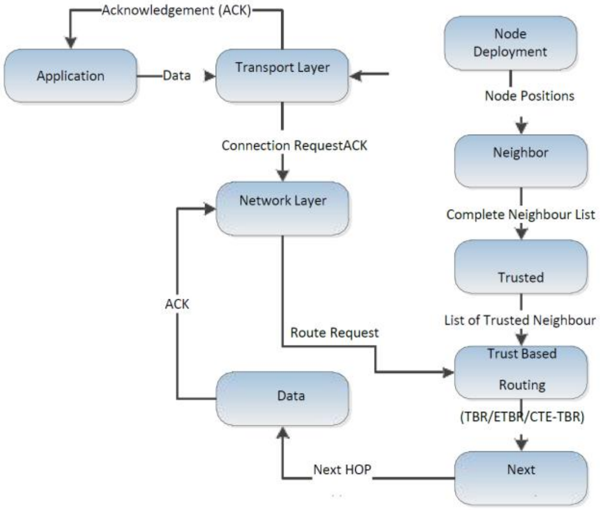


Figure 1: Block Diagram

All the 3 schemes are simulated using Network Simulator – NS2 and networking parameters like Packet Delivery Ratio (PDR), End-to-End Delay and Remaining Energy are compared. CTE-TBR is more effective than other schemes with better PDR and remaining energy.

2 Literature Review

In this section we look at the research that has been done in the area of data security in networks and specifically in WSN based data critical applications. As discussed in the previous section, the problem at hand has three parts. First part deals with trust value concept where trust value of a node is the guarantee that the node will not involve in activities like manipulating the data or injecting false data in to the network. Second part of the problem is to develop computationally less complex light weight cryptographic scheme suitable for energy constrained WSNs. Third and final part of the problem is to develop application-level security through user level authentication, session management and secured handshake between applications. Based on this, literature review also has to be focused on the above-mentioned areas and considered articles classified in to 4 categories. The categories are:

- Security issues in WSN and its countermeasures.
- Concept of trust and its applications.
- Trust value of nodes for routing.
- Different approaches for trust value computation.

Security Issues in WSN and Its Countermeasures

Many domains like healthcare, defense, surveillance etc. have benefitted largely by deploying application over Wireless Sensor Networks. The features of WSNs like mobility, scalability, dynamic topologies etc. have provided better performance and reliability to applications. Many of the deployed applications are data critical and security of data is very essential. Various attacks aim at WSN and Black

Hole attacks, Sink Hole attacks, False Data Injection attacks etc. are some of the most widely noticed attacks on WSN based applications.

In the paper (Bangotra, D.K., 2022), author list out the various attacks which aim at WSN based applications and critically reduces the data security of these applications. The survey summarize that cryptographic schemes are the most common solutions to attacks on WSN. The paper also discusses about various categories of cryptographic schemes like private key cryptography and public key cryptography etc. In paper (Mahamune, A.A., 2021), the authors list out the various types of attacks on WSN and briefs that wormhole attacks are the most dangerous category of attacks. The authors suggest a solution using a modified AODV routing protocol-based approach to eliminate wormhole attacks. (Khan, T., 2021) discusses the various attacks on network applications and categorize them based on which layer the attack takes place. In paper (Xu, Q., 2021), various security attacks are summarized and categorize them as Man-in-the-Middle attacks and Malicious Node attacks. (Singh, S., 2019) lists out the various security challenges in WSN and cryptographic techniques for keeping the data secure. The paper proposed a technique called Sensor Network Encryption Protocol (SNEP).

Concept of Trust and Its Applications

In spite of the advantages of WSN, applications lack data security as the nodes in WSN are energy constrained devices and when energy dries up for a node, it may lead to network partitioning. Traditionally data security in network applications are devised with the help of cryptographic schemes. Cryptographic solutions are computationally complex and requires higher quantity energy utilization from individual nodes. This makes cryptographic solutions not the best possible solution. An alternative solution suggested by most of the researchers is the idea of trust.

(Desai, S.S., 2021) present a concept of 'Trust of a node'. According to the authors, trust value of a node is the guarantee that the node will not be involved in any of the activities which damages the data security. The paper list the various domains where trust value concept can be applied. In (Farruh Ishmanov, 2017), Tian et. al. discusses about the computation of trust value of a node. The author suggests the possible parameters that can be considered for computation of trust value of a node. The parameter list includes delay, packet delivery ratio, range of transceiver devices etc. In paper (Archana Sharma, 2019), the authors suggest the use of trust value of a node for routing purpose. The idea is to categorize nodes as trusted nodes and malicious nodes. Malicious nodes will have low trust value. (Bangotra, D.K., 2022) proposes a trust-based scheme for Cluster based WSN. The authors propose energy as a parameter for trust computation as low energy level of a node indicates its inability to forward packets effectively. (Sumalatha, M.S., 2021) discusses the possibility of using trust in cluster-based systems. The authors propose a 2-layer trust-based security scheme for Cluster based Intrusion Detection systems. The trust value computation takes place at both cluster member level and cluster head level. In (Zhao, J., 2019), the authors point out a specific attack in which certain nodes intentionally drops packets to reduce the packet delivery ratio and increase the retransmissions which will eventually result in energy depletion.

Trust Value of Nods for Routing

Ansari et. al. proposes trust value for routing in (Terence, J.S., 2019) where forwarding is based on the trust value of neighboring nodes. The neighbor node with highest trust value is considered for forwarding the packet. (Dewal, P., 2018) summarizes the various schemes researchers have proposed which uses trust value for routing and the authors list the challenges which still exists in those systems. The major challenges notified by the authors include lack of proper mathematical model for trust computation, weak selection of parameters for trust value computation etc. (Momani Mohammad, 2010) propose an opportunity-based routing scheme that uses trust value of a node. The paper also introduces the concept of trust and reputation. Reputation of a node is similar to trust value, but it is calculated by the neighbors of the node. (Khan, T., 2019) introduces a term trust-based forwarding in which the AODV routing algorithm is modified by including trust value is another parameter for deciding the next forwarding node. (Faris Fazlic, 2019) suggests an extended routing mechanism suggested in (Momani Mohammad, 2010). The enhanced routing scheme suggests a weighted calculation of trust value of a node. The authors of (Bade, A.M., 2019) attempts to use the concept of trust in MANETs. This attempt is unique due to the fact that it is one of the first attempt to consider trust of a node in MANETs and also the fact that in the proposed system, trust value is used in transport layer rather than network layer. Tayyab et. al. (Varsha G., 2017) proposes a mathematical model for trust computation in which the trust value of a node reduces exponentially on every packet drop.

Different Approaches for Trust Value Computation

(Ansari, 2017) attempts to propose a trust-based data security scheme and compare it against traditional cryptographic schemes. The results indicate that trust-based scheme is computationally less complex and thus present itself as an effective data security scheme for WSN based applications. (Oke, J.T., 2018) discusses about a mathematical model based on exponential model for trust computation. The proposed scheme considers few parameters like Packet Delivery Ratio (PDR), End-to-End Delay. The authors propose to use throughput to individual destinations to compute trust. (Kahina Chelli, 2015) proposes different aspects of trust like authentication-based data trust, scheduler-based node trust, and attack resistant. (Hong Zhong, 2016) consolidates various trust evaluation models like weighted sum, binary, probability-based trust evaluations. The authors suggest Probability based trust estimation as the effective scheme as it considers multiple parameters. (Amol R. Dhakne, 2016) proposes a cross layer security scheme called Cross layer security based fuzzy trust calculation mechanism (CLS-FTCM). The proposed system uses 4 levels of trust such as Direct Trust, Indirect Trust, Recommendation Trust and Past Trust. (Sreevidya, B., 2018) (Sreevidya B., 2020) also discuss about the concept of trust and its computation. (Rajesh M., 2017) discuss the energy optimization in routing process while (Sreevidya, B., 2018) discuss about cryptographic scheme for data security. (Sreevidya, B., 2018) introduces the false data injection attacks and its countermeasures.

Summary of Literature Survey and Research Gaps

There has been good amount of research made on Wireless Sensor Networks, Energy Optimization in WSNs, but not much of focus was on data security in WSN based applications (Kang, J., 2019). Due to the increased use of WSN and IoT technologies to build efficient and smart solutions in healthcare, remote sensing, surveillance and border security domains, the necessity to have secure data transmission in the application has been the primary interest. The requirement of having secure data transmission over WSN based applications is in complete contrast with the inherent nature of WSN nodes to be designed for energy optimization. The major hurdle in providing data security to WSN based applications is the fact that the most commonly opted technique for providing data security is cryptography and most of the cryptographic schemes are computationally complex.

The need for an alternative to cryptographic schemes energy efficiency is increased multi-fold in data critical applications deployed over WSNs. The concept of trust value is proposed by researchers to cater data security, but the following points are identified lacking in the existing systems using trust value.

- Lack of proper mathematical models for trust value computation
- Weaker selection of parameters for trust value computation

- Lack of detailed analysis of effectiveness in terms of performance of various trust computation models

3 Proposed System

Based on this understanding, a routing scheme named Trust Based Routing (TBR) was developed previously which uses trust value in routing process. This system has 5 sublevels - Node Deployment, Trust Value Computation, Trusted Neighbor Listing, Trust based Routing, Secured Data Transfer. Once the nodes are deployed, each identifies its neighbors. Each node computes the trust value and it uses the following parameters:

- Remaining battery /energy
- Number of packets dropped
- Number of packets forwarded
- Delay
- Sleep cycle time
- Reputation (Neighbor provides this information).

The scheme uses the concept of indirect trust where the neighboring nodes also contribute in the trust value computation of a node. In addition to this, the inclusion of remaining battery / energy and sleep cycle time parameters are intended towards energy optimization. The trust value is computed using the weighted average sum of the parameters where weights are calculated using experimental way in which the influence of each parameter is analyzed individually.

Extended Trust Based Routing (TBR)

Based on the further literature review carried and the understandings acquired through the study, the previously proposed model is improved. The modified scheme is referred as Extended Trust Based Routing (ETBR). The major modifications carried out are:

Instead of calculating trust of a node based on its general behavior towards its neighbor nodes, the modified scheme computes trust value of a node with respect to its behavior towards another node. As trust value of a node changes with time, it is decided to include the influence of past trust in computing the trust of a node in the current time slot.

The concept of trust used in the previous scheme is a value which is computed by a node itself based on specific parameters. In the proposed system, the idea of trust is changed to accommodate the fact that trust of a node will not be same towards all neighbors and it can vary with respect to each forwarding node. For example, if node i is transmitting packet to node j, trust of node i observed and calculated by node j is represented as Tij.

Many researchers mentioned that trust value of a node is not a permanent value and it changes with time. This indicates that, when trust value is represented, the time slot also need to be specified. This leads to the modified representation of trust value as,

T^{t}_{ij} where t is the time slot in which the trust value is referred, i and j indicates that the trust value of node i is represented which monitored and calculated by node j. Since time slot of trust value is included in the representation, it makes sense to differentiate between value of trust in present time slot and trust value in previous time slot. These values are represented as:

CT^{t}_{ij} indicates Current Trust value of a node i monitored and calculated by node j at the present time slot t. PT^{t}_{ij} indicates the Past Trust value of a node i monitored and calculated by node j at a previous time slot t-1.

$$T^{t}_{ij:=\alpha\left(CT^{t}_{ij}\right)+(1-\alpha)\left(PT^{t}_{ij}\right)}$$

Consolidated Trust Estimation - Trust Based Routing (CTE-TBR)

It is identified that the trust value of a node is not alone the value computed from node's forwarding behavior like number of packets forwarded, number of packets dropped, delay etc., instead the energy consumption of the node also reveals the behavior of a node. Many researchers have used the concept of indirect trust along with the trust computed of a node to assess the behavior of a node. Based on these understanding, Extended Trust Based Routing (ETBR) scheme was further enhanced by including past trust value and modifying the way trust of a node is computed. The modified version is referred as Consolidated Trust Estimation – Trust Based Routing (CTE-TBR).

In Consolidated Trust Estimation – Trust Based Routing (CTE-TBR), trust value of a node is computed as the combination of 3 aspects – Direct Trust, Indirect Trust and Energy Trust. Direct Trust computation considers the fact that, trust value of a node changes with time and to accommodate this change in trust value, past trust value is also considered while computing the current time slot trust. While calculating Indirect Trust, the traditional approach considers only neighboring nodes, but to improve the accuracy, all the nodes are involved in the proposed scheme. To accommodate the draining energy level of a node, energy trust is considered. While computing the Consolidated Trust of a node, the 3 aspects of trusts (Direct Trust, Indirect Trust and Energy Trust) are combined using Weighted Sum approach. Weights are chosen in such a way that the influence of Energy Trust is increased as time progress.

Direct Trust (DT) is the value of trust computed by node j about node i based on its previous history and current transmission and reception activities performed. DT is the indicator of a node's guarantee that it can be considered for forwarding the packets and the packets will not be manipulated. Direct Trust is calculated as the weighted sum of Historical Trust (HT) and trust generated from Receive and Send operations as shown in Eq. 1.

$$\mathrm{DTtij} = \alpha(\mathrm{HTtij}) + (1 - \alpha)\,(R_j + S_j)^t \qquad \text{(Eq. 1)}$$

DTtij: Direct Trust of Node i computed by Node j at time t

HTtij: Historical Trust of Node i computed by Node j at time t

(Rj + Sj)t : Trust generated by the send and receive operation performed by Node i to Node j at time t.

α: Weight value which will balance the influence of both historical trust and trust generated from send & receive operations.

Historical Trust is calculated as given in Eq. 2.

$$\mathrm{HTtij} = \beta(\mathrm{DT(t-1)ij} + \mathrm{H}t\mathrm{(t-1)ij}) \qquad \text{(Eq. 2)}$$

β: Weight value which will balance the influence of historical trust on current trust.

Send & Receive Trusts are calculated as given in Eq. 3 and Eq. 4 respectively

$$\mathrm{S_j} = \frac{(send\_messagej - un\_sendj)}{messagej} \qquad \text{(Eq. 3)}$$

$$R_j = \frac{(receive\_messagej - rejectionj)}{messagej} \quad \text{(Eq. 4)}$$

receive_messagej: the number of data packets received by node j from node i.

send_messagej: the number of data packets sent by node j to node i.

messagej: the total number of data packets received and sent by node j.

rejectionj: the number of data packets that node j received but corrupted.

un_sendj: the number of data packets that node j dropped rather than forwarding.

Indirect Trust is the impression of one node on another node through the trust values of other nodes. It is computed as given in Eq. 5.

$$\mathrm{ITtij} = \frac{1}{q}\sum_{1}^{q}(\mathrm{DTtiu} + \mathrm{DTtuj}) \quad \text{(Eq. 5)}$$

To calculate the energy consumed by a node, energy consumed in sending and receiving data is calculated as given in Eq. 6, Eq. 7, Eq. 8 and Eq. 9.

$$E_{send} = L * E_{radio\_transmission} \quad \text{(Eq. 6)}$$

$$E_{receive} = L * E_{radio\_reception} \quad \text{(Eq. 7)}$$

Remaining Energy of node

$$RE_j = E_0 - E_{send} - E_{receive} \quad \text{(Eq. 8)}$$

where E0 is the initial energy.

$$Ej = \frac{REj}{E0} \quad \text{(Eq. 9)}$$

Finally, the Consolidated Trust is calculated as a weighted sum of the above mentioned 3 different categories of trust as given in Eq. 10.

$$CTtij = \eta 1 * DTtij + \eta 2 * \mathrm{I}Ttij + \eta 3 * E_j \quad \text{(Eq. 10)}$$

η1, η2, η3 are the weights of direct trust, indirect trust and energy trust, respectively and η1 + η2 + η3 = 1.

4 Implementation

The approach is implemented with NS2 using the Simulation parameters listed in Table 1 to understand the effectiveness of the proposed system. Because there are a few network simulators available to simulate network protocols and related procedures. It is preferable to simulate the proposed system rather than implement it on a real-world WSN. Network Simulator (NS2) is the most popular simulator because it is open source and free to download and use. Furthermore, NS2 includes many libraries that can support the simulation of any network and any network protocols/procedures.

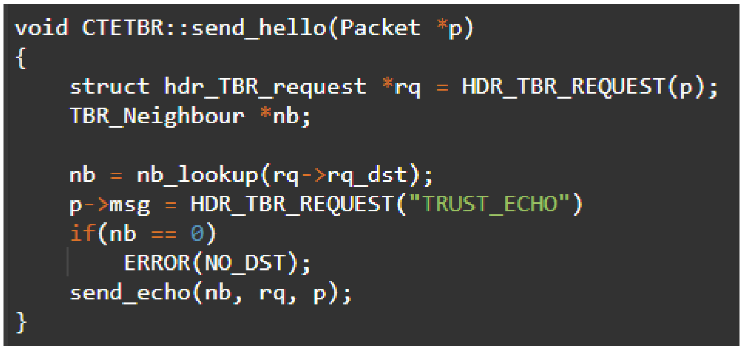
Table 1: Simulation Parameters

Parameters	Values
Simulation time	25 s
Monitoring area	100 × 100 m^2
Number of nodes	20 to 100
Propagation model	Two Ray
Packet interval	0.5 s
Length of the data packet	1000 bytes
Initial energy	100 J
Transmit power	0.9 w
Receive power	0.8 w
Idle power	0.1 w
Sense power	0.0175 w
Routing protocol	AODV (TBR)
MAC layer protocol	IEEE 802.11

The features for deploying wireless sensor nodes, the availability of AODV protocol source code, trace files for monitoring, and log generation made NS2 the best simulator for implementing the proposed system. A random deployment model available in NS2 deploys the sensor nodes. Nodes are initialized with preliminary battery energy and trust value upon deployment. Following this thread, nodes will function as regular sensor nodes, with sleep and active cycle, and data will be collected from the sensors attached during the active cycle. Each node attempts to understand the network to form and communicate the data collected. In traditional routing algorithms, nodes collect data about neighbors by sending Hello packets, and the network is built based on the responses.

To implement the proposed system where trust value is computed considering 3 aspects - Direct Trust, Indirect Trust and Energy Trust, additional modules are added to the existing code of AODV routing protocol which is already available in NS2. Modified system defines two functions, send_hello() and recv_hello(), for sending and receiving hello packets.

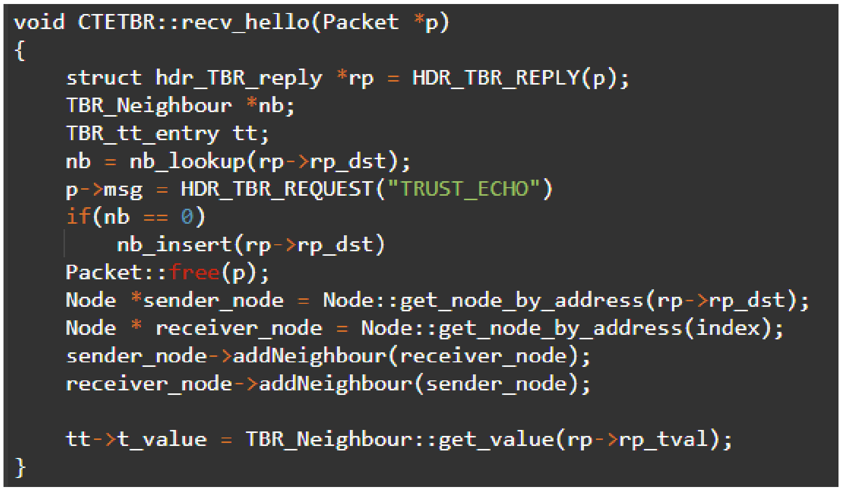
Aside from identifying the neighbor and determining the hop count of the neighboring nodes, the routing protocol in the proposed system uses echo packets to share each node's trust value. These features are defined in the node's send_hello() and recv_hello() functions.cc file. Figure 2 depicts the send_hello() function, while Figure 3 depicts the recv_hello() function.



```
void CTETBR::send_hello(Packet *p)
{
    struct hdr_TBR_request *rq = HDR_TBR_REQUEST(p);
    TBR_Neighbour *nb;

    nb = nb_lookup(rq->rq_dst);
    p->msg = HDR_TBR_REQUEST("TRUST_ECHO")
    if(nb == 0)
        ERROR(NO_DST);
    send_echo(nb, rq, p);
}
```

Figure 2: Code for send_hello() function

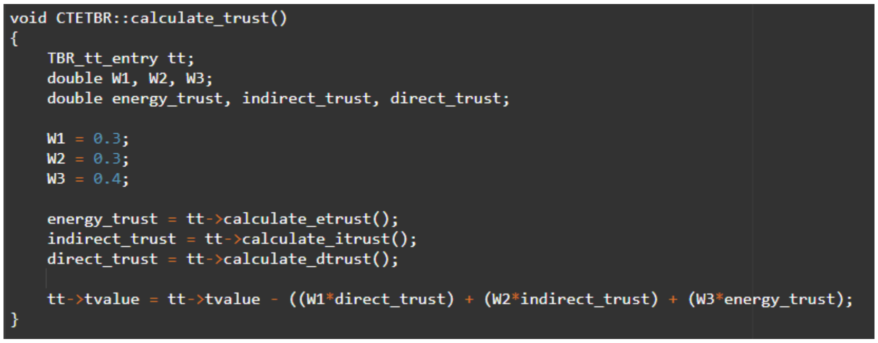


```
void CTETBR::recv_hello(Packet *p)
{
    struct hdr_TBR_reply *rp = HDR_TBR_REPLY(p);
    TBR_Neighbour *nb;
    TBR_tt_entry tt;
    nb = nb_lookup(rp->rp_dst);
    p->msg = HDR_TBR_REQUEST("TRUST_ECHO")
    if(nb == 0)
        nb_insert(rp->rp_dst)
    Packet::free(p);
    Node *sender_node = Node::get_node_by_address(rp->rp_dst);
    Node * receiver_node = Node::get_node_by_address(index);
    sender_node->addNeighbour(receiver_node);
    receiver_node->addNeighbour(sender_node);

    tt->t_value = TBR_Neighbour::get_value(rp->rp_tval);
}
```

Figure 3: Code for recv_hello() function

The send_hello() function calls the calculate trust() function, which computes the trust value using the equation equations explained above. The calculate_trust() function is shown in Figure 4. This function is also defined in the file node.cc. When the hello packet is received, the trust value of other neighbor nodes is extracted and passed to the function neighbor_list(). Figure 5 depicts the neighbour_list() function. This function finds neighbors with trust values greater than the threshold and adds them to trusted neighbors' linked list data structure. The routing algorithm uses this data structure to determine the best path.



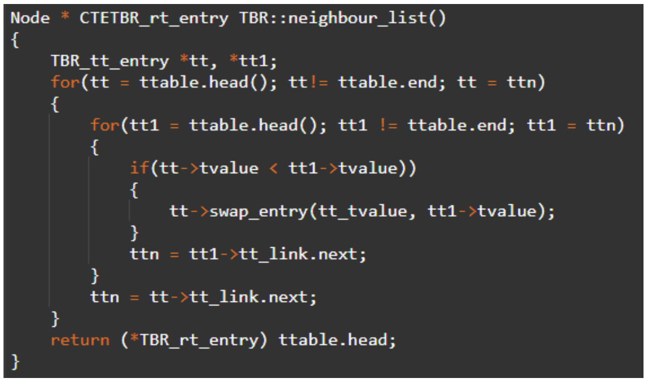
```
void CTETBR::calculate_trust()
{
    TBR_tt_entry tt;
    double W1, W2, W3;
    double energy_trust, indirect_trust, direct_trust;

    W1 = 0.3;
    W2 = 0.3;
    W3 = 0.4;

    energy_trust = tt->calculate_etrust();
    indirect_trust = tt->calculate_itrust();
    direct_trust = tt->calculate_dtrust();

    tt->tvalue = tt->tvalue - ((W1*direct_trust) + (W2*indirect_trust) + (W3*energy_trust);
}
```

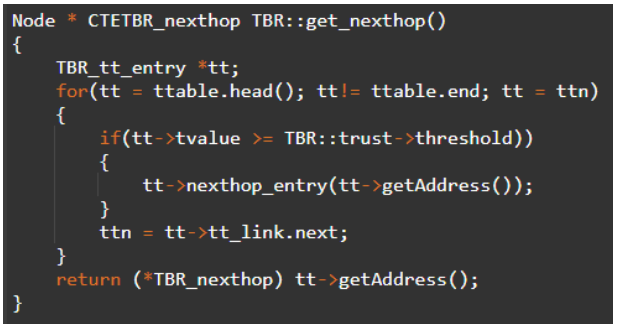
Figure 4: Code for calculate_trust() function



```
Node * CTETBR_rt_entry TBR::neighbour_list()
{
    TBR_tt_entry *tt, *tt1;
    for(tt = ttable.head(); tt!= ttable.end; tt = ttn)
    {
        for(tt1 = ttable.head(); tt1 != ttable.end; tt1 = ttn)
        {
            if(tt->tvalue < tt1->tvalue))
            {
                tt->swap_entry(tt_tvalue, tt1->tvalue);
            }
            ttn = tt1->tt_link.next;
        }
        ttn = tt->tt_link.next;
    }
    return (*TBR_rt_entry) ttable.head;
}
```

Figure 5: Code for beighbour_list() function

In the aodv.cc file, a user-defined function get_nexthop() is defined, which retrieves the trusted neighbor's list from the trusted neighbor structure stored in my_route.cc file. The get_nexthop() function is illustrated in Figure 6. This trusted neighbor list is used to determine the best path. This function returns the node that will forward the packet.



```
Node * CTETBR_nexthop TBR::get_nexthop()
{
    TBR_tt_entry *tt;
    for(tt = ttable.head(); tt!= ttable.end; tt = ttn)
    {
        if(tt->tvalue >= TBR::trust->threshold))
        {
            tt->nexthop_entry(tt->getAddress());
        }
        ttn = tt->tt_link.next;
    }
    return (*TBR_nexthop) tt->getAddress();
}
```

Figure 6: Code for get_nexthop()

In route.cc, a user-defined function route_update() is defined, assigning the next-hop address for each packet to arrive at the destination. This function calls get_nexthop() to determine the next node to which a packet should be forwarded. Based on the get_nexthop() function, the routing algorithm forwards the packet to the neighbor while avoiding the compromised nodes. Following the identification of the next hop, the node forwards the packet using simple cryptographic encryption. Because the trusted neighbor list generation phase occurs before the Routing, compromised nodes are avoided. All attacks from compromised nodes will be avoided as a result. Furthermore, the trust-based routing scheme does not frequently broadcast echo packets, reducing energy consumption. This will improve the system's energy efficiency. The final encryption scheme improves data confidentiality.

5 Results and Discussion

Only when compared to other similar approaches, can the effectiveness of the proposed system be demonstrated. As a result, the proposed method's performance is compared to two parallel approaches. The first is the Trust Based Routing (TBR) scheme developed previously. The second is a variant of the TBR scheme suggested by modifying the concept of past trust and concept of trust computation. This model is referred as Extended Trust Based Routing (ETBR). Three WSN network parameters are compared to analyze performance and validate the claim that the proposed system is energy efficient: throughput, packet delivery ratio, and remaining battery energy. The details are not provided because Delay, Packet Delivery Ratio, and Remaining Energy are standard network parameters.

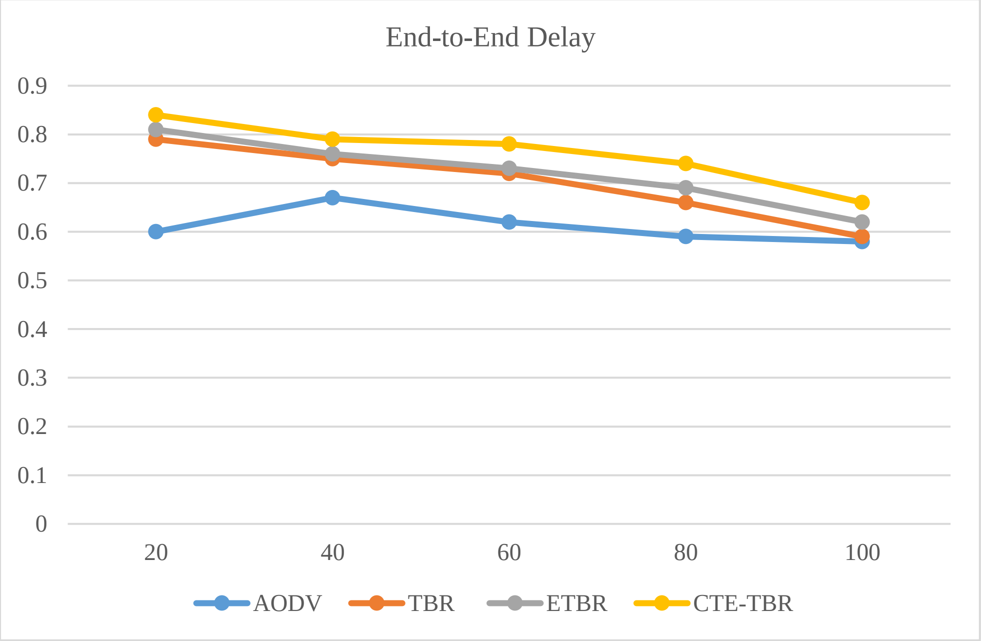


Figure 7: Delay Comparison

Figure 7 compares traditional AODV-implemented WSN, Trust Based Routing (TBR) Scheme-based WSN, Extended Trust Based Routing (ETBR) and the proposed system in terms of delay. The proposed system has a longer delay than the other schemes due to the fact that more computation is required in the initial stage, but it eventually improves and performs similarly to the other schemes. The long initial delay is caused by the number of times nodes compute their trust value and gather the trust value of their neighbors.

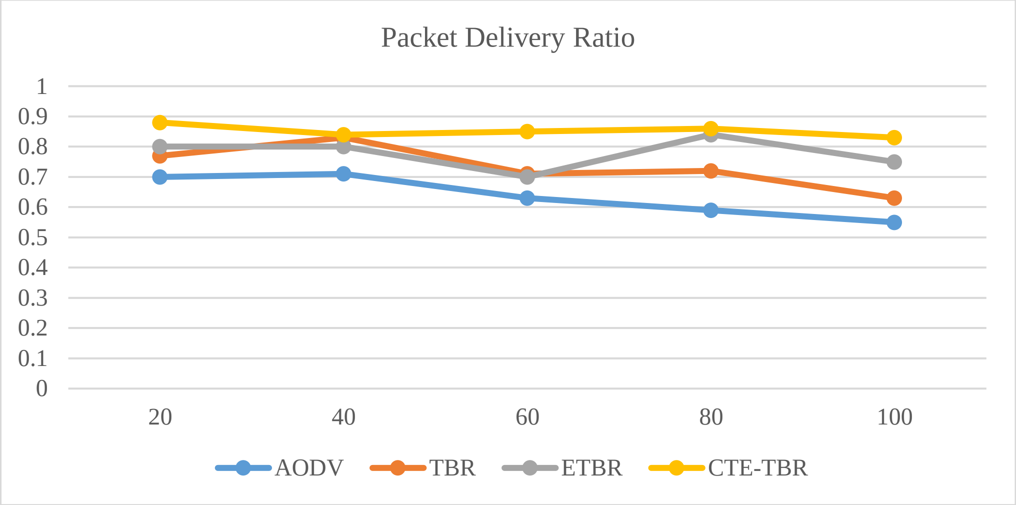


Figure 8: Packet Delivery Ratio Comparison

In Packet Delivery Ratio, Figure 8 compares traditional AODV-implemented WSN, Trust Based Routing (TBR) Scheme-based WSN, Extended Trust Based Routing (ETBR), and the proposed system. The proposed system's PDR improves over time and outperforms the other methods.

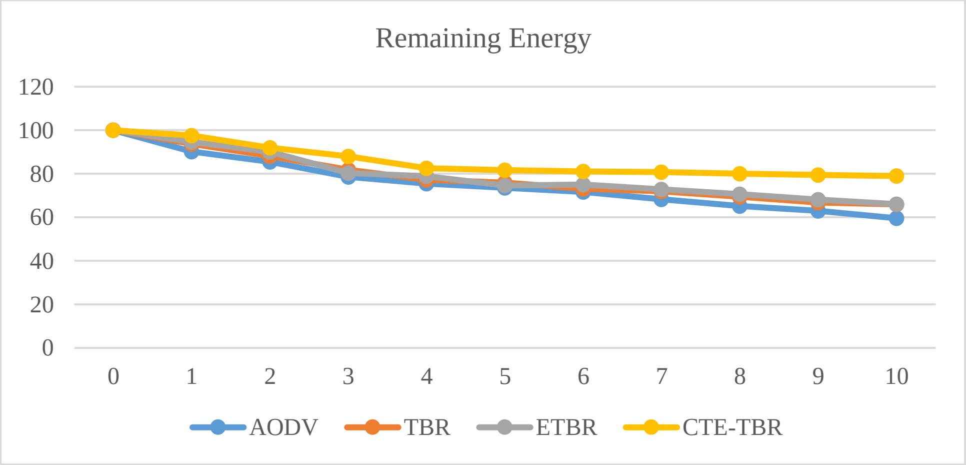


Figure 9: Remaining Battery Energy Comparison

Figure 9 compares traditional AODV-implemented WSN, Trust Based Routing (TBR) Scheme-based WSN, Extended Trust Based Routing (ETBR), and the proposed system in terms of remaining battery energy. Because the proposed method is computationally simple and consumes less power, the remaining battery energy of the proposed system is always greater than that of the other schemes. Furthermore, all the trust-based Routing schemes explained in the work are energy-efficient routing technique because it broadcasts fewer echo packets.

6 Conclusion

This paper proposes a novel data security scheme based on trust value computation to remove compromised nodes from decision-making and modify data transmitted across the WSN. The work illustrates 3 models – Trust Based Routing (TBR) which uses a weighted sum approach to compute the trust, Extended Trust Based Routing (ETBR) where past trust is used, and Comprehensive Trust

Estimation – Trust based Routing (CTE-TBR) which uses past trust concept, indirect trust, energy trust etc. The proposed scheme is a non-cryptographic scheme that employs a trust value for each node, with the trust value serving as the metric for identifying compromised nodes. Because the proposed scheme is non-cryptographic, it is less computationally complex than the most well-known cryptographic schemes used for data security, and thus it is energy-efficient. The Network Simulator (NS2) is used to simulate the proposed system models. The results show an increase in network lifetime by lowering the energy consumption of the data security scheme. The proposed system considers several parameters when calculating trust values. A scheme is a weighted approach, including more parameters and reviewing the weighted scheme of parameters in the trust value computation.

References

[1] Amol, R.D., & Prashant, N.C. (2016). TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network. *IJCSNS International Journal of Computer Science and Network Security*, *16*(12), 01-10.

[2] Archana, S., Yashwant, S., & Nagesh, K. (2019). Trust and Reputation based Secure Opportunistic Routing Protocol for WSN. *International Journal of Advanced Science and Technology*, *28*(19), 834-846.

[3] Awais, A., & Gouri, P. (2017). A Novel Composite Routing Strategy to Enhance Trust and Network Lifetime in WSN. *International Journal of Advanced Technology and Innovative Research*, *9*(7), 1224-1231.

[4] Bade, A.M., & Garba, A.A. (2019). A Review on Security Issues in Wireless Sensor Networks. *International Journal of Recent Academic Research*, *1*(5), 159-164.

[5] Bangotra, D.K., Singh, Y., Selwal, A., Kumar, N., & Singh, P.K. (2022). A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. *Wireless Personal Communications*, *127*(2), 1045-1066.

[6] Chelli, K. (2015). Security issues in wireless sensor networks: Attacks and countermeasures. *In Proceedings of the world congress on engineering*, *1*(20), 876-3423.

[7] Costa, G., Lazouski, A., Martinelli, F., Matteucci, I., Issarny, V., Saadi, R., & Massacci, F. (2010). Security-by-Contract-with-Trust for mobile devices. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *1*(4), 75-91.

[8] Desai, S.S., & Nene, M.J. (2021). Multihop trust evaluation using memory integrity in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, *16*, 4092-4100.

[9] Dewal, P., Narula, G.S., Jain, V., & Baliyan, A. (2018). Security attacks in wireless sensor networks: A survey. *In Cyber Security: Proceedings of CSI 2015*, 47-58.

[10] Fazlic, F., Hashemi, S.A., Aletic, A., Abd Almisreb, A., Norzeli, S.M., & Din, N.M. (2019). A survey on security in wireless sensor network. *Southeast Europe Journal of Soft Computing*, *8*(1), 35-41.

[11] Ishmanov, F., & Bin Zikria, Y. (2017). Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues. *Journal of Sensors*, *2017*. https://doi.org/10.1155/2017/4724852

[12] Kang, J., Kim, J., & Sohn, M.M. (2019). Supervised learning-based Lifetime Extension of Wireless Sensor Network Nodes. *Journal of Internet Services and Information Security (JISIS)*, *9*(4), 59-67

[13] Kaur, M., & Mahajan, M. (2013). Using encryption algorithms to enhance the data security in cloud computing. *International Journal of Communication and Computer Technologies (IJCCTS)*, *1*(2), 130-133.

[14] Khan, T., & Singh, K. (2019). Resource management based secure trust model for WSN. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(8), 1453-1462.

[15] Khan, T., Singh, K., Hasan, M.H., Ahmad, K., Reddy, G.T., Mohan, S., & Ahmadian, A. (2021). ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. *Future Generation Computer Systems*, *125*, 921-943.

[16] Mahamune, A.A., & Chandane, M.M. (2021). An efficient trust-based routing scheme against malicious communication in MANET. *International Journal of Wireless Information Networks*, *28*(3), 344-361.

[17] Momani Mohammad, Subhash Challa (2010). Survey of Trust Models in Different Network Domains. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 1*(3), 1-6.

[18] Oke, J.T., Agajo, J., Nuhu, B.K., Kolo, J.G., & Ajao, L.A. (2018). Two layers trust-based intrusion prevention system for wireless sensor networks. *Advances in Electrical and Telecommunication Engineering*, *1*, 23-29.

[19] Ram, A., & Chakraborty, S.K. (2024). Analysis of Software-Defined Networking (SDN) Performance in Wired and Wireless Networks Across Various Topologies, Including Single, Linear, and Tree Structures. *Indian Journal of Information Sources and Services, 14*(1), 39–50.

[20] Singh, S., Ra, I.H., Meng, W., Kaur, M., & Cho, G.H. (2019). SH-Block CC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*, *15*(4), 01-18.

[21] Sreenivasu, M., Kumar, U.V., & Dhulipudi, R. (2022). Design and Development of Intrusion Detection System for Wireless Sensor Network. *Journal of VLSI Circuits and Systems*, *4*(2), 1-4.

[22] Sreevidya, B., & Rajesh, M. (2017). Enhanced energy optimized cluster based on demand routing protocol for wireless sensor networks. *In International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2016-2019.

[23] Sreevidya, B., & Rajesh, M. (2018). False data injection prevention in wireless sensor networks using node-level trust value computation. *In IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2107-2112.

[24] Sreevidya, B., & Supriya, M. (2020). Malicious Nodes Detection and Avoidance using Trust Based Routing in Data Critical Wireless Sensor Network Applications. *Journal of Jilin University*, *16*(4), 467-478.

[25] Sreevidya, B., Rajesh, M., & Mamatha, T.M. (2018). Design and development of an enhanced security scheme using RSA for preventing false data injection in wireless sensor networks. In *Ambient Communications and Computer Systems: RACCCS*, 225-236.

[26] Sumalatha, M.S., & Nandalal, V. (2021). An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN). *Journal of Ambient Intelligence and Humanized Computing*, *12*, 4559-4573.

[27] Terence, J.S., & Purushothaman, G. (2019). A novel technique to detect malicious packet dropping attacks in wireless sensor networks. *Journal of Information Processing Systems*, *15*(1), 203-216.

[28] Varsha G., Mahesh P., Jitendra A. (2017). A Literature Survey on Security Issues of WSN and Different Types of Attacks in Network. *Indian Journal of Computer Science and Engineering*, *8*(2), 80-83.

[29] Xu, Q. (2021). Wireless sensor networks secure routing algorithm based on trust value computation. *International Journal of Internet Protocol Technology*, *14*(1), 10-15.

[30] Zhao, J., Huang, J., & Xiong, N. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. *IEEE Access*, *7*, 33859-33869.

[31] Zhong, H., Shao, L., & Cui, J. (2016). A lightweight and secure data authentication scheme with privacy preservation for wireless sensor networks. *In International Conference on Networking and Network Applications (NaNA)*, 210-217.

Authors Biography

Ms.B. Sreevidya. currently serves as Assistant Professor (Senior Grade) at Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, India. She is currently pursuing his Ph.D. She has been with Amrita University for more than 17 years now. She pursued his Master's in Computer Science and Engineering from Visveswaraiah Technological University, Bengaluru. Her area of interest includes Sensor Networks, Wireless Networks and Data Security. She has around 15 publications in the domain of wireless sensor networks and data mining. Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India.

Dr.M. Supriya, currently serves as Associate Professor at Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, India. She has been with Amrita University for more than 18 years now. Her area of interest includes Cloud Computing, Distributed Systems and Computer Security. She has around 30+ publications in the domain of cloud computing and distributed systems. Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India.