International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212555 Volume 9, Issue 3, May – June (2022)

RESEARCH ARTICLE

Trust-Based Co-Operative Cross-Layer Routing Protocol for Industrial Wireless Sensor Networks

Manish Panchal
Department of Electronics and Telecommunication, Shri G S Institute of Technology and Science Indore, Madhya Pradesh, India
hellopanchal@gmail.com

Raksha Upadhyay
Department of Electronics and Telecommunication, Institute of Engineering and Technology, DAVV Indore, Madhya Pradesh, India
raksha_upadhyay@yahoo.co.in

Prakash Vyavahare
Department of Electronics and Telecommunication, Shri G S Institute of Technology and Science Indore, Madhya Pradesh, India
prakash.vyavahare@gmail.com

Received: 11 March 2022 / Revised: 08 May 2022 / Accepted: 11 May 2022 / Published: 28 June 2022

Abstract – One of the significant applications of wireless sensor networks is Industrial Wireless Sensor Network (IWSN). These IWSNs are set up in manufacturing premises for security, manufacturing administration, data collection, and control, etc. The measured data is transmitted from the nodes to the administrative controller and data analysis systems in such networks. Real-time communication and data reliability are the two major concerns that need trusted relay nodes for further data transfer. Most of the trust-based routing protocol models in IWSN are based on detecting misbehavior at the network layer only. These approaches result in higher values of false-positive rate since the normal failure of nodes is considered as low trusted nodes. Trust-based Co-operative Cross-layer Routing Protocol (TCCRP) for IWSN is proposed in this paper to reduce the false-positive rate and for QoS parameters improvement. It consists of three phases: trust collection, trust verification, and trust evaluation. Simulation results of the proposed TCCRP protocol show the performance improvement in QoS parameters in terms of throughput, packet delivery ratio, and residual energy with a lesser false positive rate compared to the trust management-based secure routing scheme in an industrial wireless sensor network with fog computing (TMSRS).

Index Terms – WSN, Cross-Layer Design, Trust-Based Routing, QoS, False-Positive Reduction, Cooperative Routing.

1. INTRODUCTION

Continuous revolution in industrial automation set a new paradigm in industrial automation, and it depends upon new emerging technologies like IoT and Industrial wireless sensor networks (IWSN). Industrial revolution 4.0 has also emphasized automation with less human intervention in the manufacturing industries [1-3]. IWSNs are primarily utilized for gathering and transferring data from field devices. The fundamental processes of these kinds of networks are periodic measurements, data congregation, and data broadcast by discrete sensors to Base Stations (BS) through intermediate nodes. The BS gathers data and transfers it to the Control Center (CC). IWSNs have numerous benefits over conservative wired manufacturing networks, such as flexible and fast infrastructure setup, early troubleshooting, and faster reconfiguration. These IWSNs are increasingly set up in manufacturing arenas for production administration, monitoring, data attainment, and raising alerts for security concerns.

The measured data is transmitted from the nodes to an administrative controller and data collection systems for monitoring and regulatory functions in such a network. The central manager can regulate the manufacturing progressions based on data interpretations or directly instruct an on-site worker [4]. Industrial wireless sensor networks are also helpful in smart city developments. A smart city requires accurate data analysis of massive data for faster decision-making. Figure 1 shows an architecture of a typical IWSN. It comprises many minor sensors and numerous base stations (BSs) or sinks. Typically sensor nodes in IWSN communicate with BS over a wireless link such as mobile networks or satellite links. Device nodes are frequently positioned in unattended unreceptive manufacturing zones in these networks.

RESEARCH ARTICLE

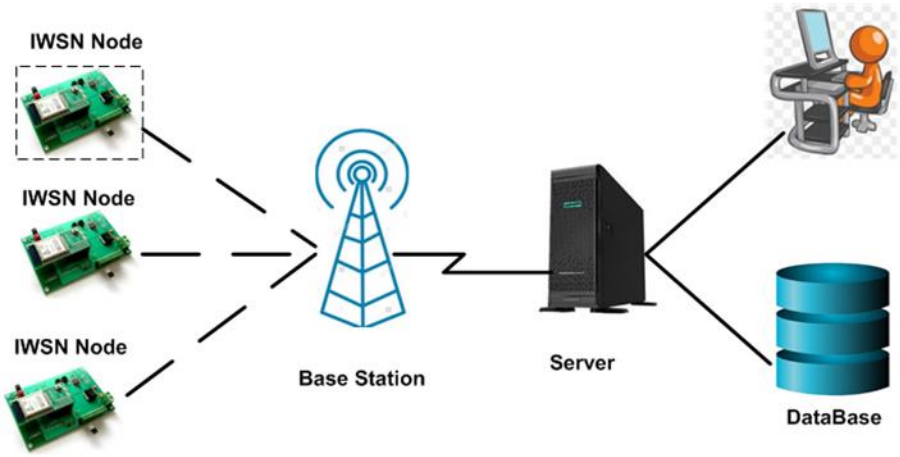


Figure 1 Typical IWSN Architecture

Moreover, these IWSNs operate in enormously complex situations with extreme necessities. Hence safety must be considered during the node deployment phase for accurate data collection.

The lack of the physical safety of sensor nodes may attack the entire network by interlopers [5-6]. Further, a faulty node producing a false reading while the event did not occur is called a false positive or vice versa for a false negative when the event was not detected [7]. With the rapid growth of the Industrial Internet of Things (IIoT), it is desirable to provide lifetime security to industrial sensor nodes [8]. However, wireless sensor network systems can be easily attacked by hackers/attackers through DDoS or by some network abnormalities at the network layer in the form of device misbehave attacks.

In DDoS, attackers compromise nodes to get information or by disturbing the normal transmission activity of the sensor to affect production/observations. The attacker can also compromise any node for information tampering, illegal routing, message injection, or making a node replica [9]. Another major issue in working with the IWSN is routing. Routing is a principal activity in the IWSNs for data communication from source to destination because of the intrinsic features of many distributed low power nodes over a large area [10]. Owing to the exposed, distributed, and active nature of IWSNs, the routing procedures are extremely susceptible to several attacks. Recently, diverse, safe routing procedures have been followed to guard IWSNs against malevolent hackers. However, these routing procedures mainly depend on cryptographic principles and verification mechanisms that are computationally intensive and, hence, inappropriate for IWSNs. Conservative safety routing procedures centered around cryptographic principles can prevent certain kinds of exterior attacks, but they cannot offer protection against malevolent conduct of interior nodes. Trust management is an effective solution to address these concerns and could be an appropriate measure for the safety design of IWSNs [11].

Trust-based routing protocols are used in WSN and ISWN. However, they are only based on protection against misbehavior at the network layer. Although such protocols consider energy as one of the routing metrics, the energy drain rate or power dissipation caused due to abnormal activities should also be considered while evaluating their performance. These approaches result in increased false positives. Therefore, normal failures of nodes can also be considered low-trusted nodes.

This paper proposes a Trust-based cooperative cross-layer routing protocol (TCCRP) characterized by trust-based routing, the false-positive rate of nodes, and the energy efficiency of IWSN. The proposed Trust-based Co-operative Cross-layer Routing Protocol **(**TCCRP) model is a cross-layer-based model where the physical, data link, and network layers work in collaboration to calculate the trust. The trust is calculated in various phases for routing, like trust collection, verification, and evaluation phases. The physical layer is considered for the residual energy of sensor nodes for energy efficiency. Routing at the network layer is based on trust calculations performed by nodes. The Trust of a node is determined and updated periodically by factors including data forwarding rate, data forwarding time, and residual battery capacity. Packets are routed using nodes having the highest trust value and the minimum hops.

Simulation has been done in DDoS and device misbehave attack scenarios. Performance has been observed through various QoS parameters such as throughput, packet delivery ratio, false-positive rate, and residual energy. In the case of a DDoS attack, the proposed TCCRP protocol shows the performance improvement in throughput by 22.8%, Packet delivery ratio by 46%, residual energy by 3%, and reduction in false-positive rate by 74%. In case of a device misbehave

RESEARCH ARTICLE

attack, the proposed protocol shows performance improvement in throughput by 70%, residual energy by 19%, and reduction in false-positive rate by 68% with reference to the TMSRS protocol.

The rest of this paper is organized as follows. Section 2 describes a literature survey of the work done in a related area. Section 3 presents the proposed approach of the TCCRP protocol, including cross-layer architecture and a trust-based routing mechanism. This section also explains finding the optimum secure route for information transfer between source to destination. Section 5 compares simulation results of the proposed TCCRP protocol with the TMSRS protocol, and its QoS parameters performance is investigated. Finally, the paper is concluded in section 5.

2. RELATED WORK AND CONTRIBUTION

Wireless sensor networks are affected in terms of functionality by various types of attacks majorly, including DDoS, misbehave, and wormhole attacks. Wormhole attack affects the routing, so to minimize the effects of this attack, NTOM-DA protocol is proposed by authors in [12], which is based on trust exchanges. Improvement in routing and the false positive rate are observed by NTOM-DA protocol with negligence precautions from other attacks. Authors in [13] proposed the ABAS protocol to handle the various jamming attacks caused by DDoS attacks. ABAS is implemented on the basis of a block-chain concept, but the issue of devices misbehave at the network layer is not covered in it. Authors in [14] discuss fault data injections and malicious node issues. The proposed strategy is based on time and spatial correlation, with the limitation of handling only certain numbers of malicious nodes. In the case of increasing numbers of malicious nodes, the false-positive and false-negative rates will be affected.

Y.Han et al.[15] proposed genetic algorithm-based protocol TAGA to cater to energy efficiency issues and secure trust routing of wireless sensor networks. Trust calculation is calculated by incorporating direct and indirect trust. TAGA outperforms well in tackling various routing attacks, and it is energy efficient with the limitation that false-positive rate issues are not handled by it. Another trust estimated secure routing ETERS had been proposed by authors [16], which consists of multiple trusts like communication, energy, and data trust. The proposed ETERS protocol may be used in the industry to handle sensitive data, but ETERS lacks the false-positive rate of sensor networks for industrial applications. The authors presented trade-offs between available resources and security issues in [17], in which a multiple dimension trust scheme was proposed. Security aspects are solved through the cryptography process, and numerous trust calculations tackle resource efficiency. However, excessive calculations in the encryption process will lead to battery power drainage, making it less energy efficient. Apart from industry and IoT, the wireless sensor networks are used in underwater applications named as UWSN. Authors in [18] analyzed the various security aspects of UWSN and the possibilities of all the layer by layer attack well in the article.

Fang et al. [19] proposed a Trust-based Security System (TSS) for the smart city which calculates the trust of nodes based on a binomial distribution. Additionally, a secure routing scheme is also presented, but this work cannot identify and cope with internal attacks. The authors have proposed CLS-FTSM [20]. It gives better results than Cross-Layer Based Security intrusion detection system (CLS-IDS). CLS-IDS is energy efficient and has a better network lifetime while CLS-FTSM provides better performance than CLS-IDS by reducing the overhead to save energy consumption. Since this work is based on fuzzy logic, more energy may be required during its practical implementation and hence is not suitable for IWSN.

Chuanyi Liu et al. [21] have suggested FRAT protocol for reckless trust computing systems centered around cross-checking procedures for grouped WSNs. The protocol has a resource-conserving trust evaluation system for collaboration among group heads or members. This system is appropriate for WSN as it eases resource-saving. However, in this FRAT protocol, node mobility and flat topology of WSN are not considered.

In IWSN, some of the major challenges are the requirements of high reliability and low real-time delay in delivery. URLLC protocol has solved these issues in [22] by introducing a special-purpose channel responsible for the transmission and reception of short superframes. URLLC can be used in Industrial Wireless Sensor networks with 5G technology. However, throughput is limited to the number of RC channels. Authors in [23] have suggested Trust Assisted Global and Greedy Congestion-aware Data Aggregation (TAG-GCDA) algorithm which offers the advantages of higher packet delivery ratio and better energy efficiency. The authors evaluated all the major QoS issues, but false-positive issues were not addressed in their proposal. For the Peer to Peer (P2P) network, TMCQA protocol is developed in which the data reporter plays a significant role. The trust value of every data reporter is calculated with a machine learning time decay function.

The improvement rate due to TMCQA in QoS performance was observed to be around 49.39% [24]. However, it is suitable for P2P networks, not for industrial WSN, which has to cover a longer sensing range. Energy consumption protocols like EERS have been suggested, reducing the number of synchronization and scheduling messages. It also increases the performance of the scheduling process [25]. The limitation of this protocol is that simulation is dependent upon the larger set of reference nodes, which is not optimum.

RESEARCH ARTICLE

Ghugar et al. proposed the LB-IDS in [26] to detect malicious nodes in clustered WSNs. In LB-IDS, a trust value is derived uniquely for each SN at the three most promising attacking layers: physical, MAC, and network. The trust values of direct and indirect nodes are considered, and deviation in the trust value is computed. The calculated trust value is then sent to the cluster head which will decide whether the node is genuine or not. However, with the increase in the number of neighboring nodes, the message complexity and energy consumption also increase. The Trust Management-based Energy Efficient Routing Scheme is proposed by Fang et al. [27] for IWSN to maintain the security trade-off based on trust value, residual energy, and transmission performance. However, in the throughput calculation, many important overhead messages are neglected. Liu et al. [7] have suggested TPE-FTED is to manage reliability and data redundancy properly. Protocol especially developed for IWSN in which sensor nodes are deployed in a harsh situation where human innervation is not feasible. This protocol will notify the controlling unit about false-positive nodes. The protocol is based upon the extraction of trajectory patterns. However, the scheme is most suitable for industrial applications, not for normal WSNs.

Yu et al. [5] mentioned a trust computing algorithm with binomial distribution cum filter method which further improves the trustfulness, reliability, and robustness under critical conditions of industrial environments. Yang et al. [28] have suggested an energy optimal secure routing protocol centered around a disseminated trust assessment model to recognize and separate malicious nodes. This routing procedure adopts a multi-objective routing policy, considering the node's trust level, the enduring energy, and track distance. This plan confirms that data is transferred via reliable nodes and saves energy ingestion among the reliable nodes.

2.1. Problem Statement

As per the industry 4.0 standard, there is a strict requirement to automate and monitor industry-sensitive events through IWSN and its relevant sensors. Sensors deployed in the industry are primarily based on event-driven. Hence their response to that event is very critical. But sometimes, due to lack of security and in a network attack scenario, they will produce unnecessary responses while the event doesn't occur, which is called a false positive. This false positive will lead to unnecessary panic in the industrial process. Moreover, wireless networks are susceptible to distributed denial-of-service and device misbehave attacks. These attacks will try to drain out the batteries due to the execution of unnecessary events inside IWSN nodes, which shortens the battery life. Therefore, considering the limitations of existing protocols of IWSN, the main objectives of this proposed protocol are as follows:

(i) It should reduce the false positive rate

(ii) It should result in reduced computation and communication overhead than existing proposals and therefore preserve the residual battery power.

(iii) The countermeasure mechanisms through trust-based routing should also mitigate abnormalities that may occur at other layers due to various reasons.

3. PROPOSED TRUST-BASED PROTOCOL

The proposed Trust-based Co-operative Cross-layer Routing Protocol (TCCRP) combines cross-layer modeling between network, MAC and physical layers and trust-based routing decisions in wireless sensor networks. The objective of the proposed routing protocol is to offer an integrated solution for improvement in QoS parameters like throughput, Packet Delivery Ratio, Residual energy and reduction in false-positive rate for industrial wireless sensor networks.

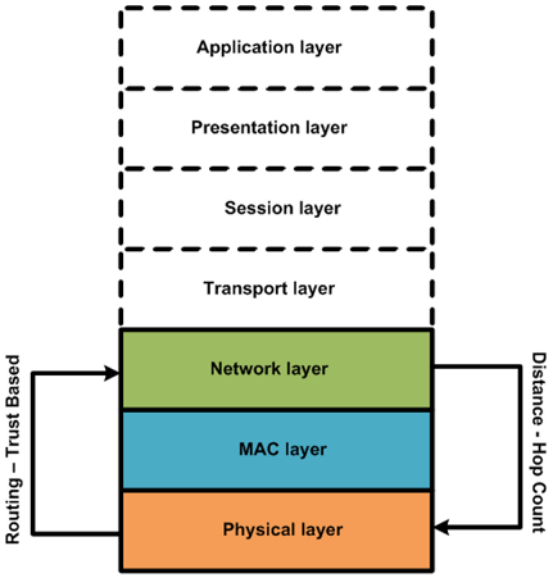


Figure 2 Proposed Cross-Layer Model

In TCCRP Protocol, network and MAC layers work in association to offer trust values to nodes in IWSN. In the proposed protocol, emphasis has been given to the physical, MAC, and Network layers to satisfy and provide a better solution for improvement in QoS parameters. As shown in Figure 2, the physical layer is considered for residual energy of sensor nodes for energy efficiency as one of the parameters in this proposed architecture. Network layer routing is based on trust calculations done by nodes. Trust is based on various factors such as data forwarding rate, data forwarding time and residual battery capacity. Routing of packets is done based on the highest trust and lowest hop count basis. The Cross-layer model is simulated through variations in the network and physical layer parameters to determine optimized parametric value in a given situation. To meet the above-said objectives, we proposed a cross-layer-based cooperative trust

RESEARCH ARTICLE

routing protocol for IWSN. The protocol is developed as an extension of the IEEE 802.15.4 WirelessHART Network. As shown in Figure 3, the proposed TCCRP consists of the following three phases: (i) Trust collection phase, (ii) Trust verification phase, and (iii) Trust evaluation phase. All these phases are shown in Figure 3.

Figure 3 Trust Mechanisms in Proposed TCCRP Approach

Trust Collection Phase: Direct Behavioral Trust (DBT) of each node is estimated based on the forwarding rate of packets, forwarding time of packets and energy dissipation rate at the node. The forwarding rate and forwarding time are determined for both data and control packets. The control packets are originated from routing and MAC layers. The energy dissipation rate is estimated at the physical layer. The source broadcasts a TRUST_COLLECTION_REQ (TCR) message to the field devices in the trust collection phase. The typical frame format of TCR is shown in Table 1. On receiving this request, each device N_i estimates the Direct Behavioral Trust (DBT) of its neighbors.

Table 1 Format of TR_COLL_REQ

Node ID	Hop Count	DFR	DFT	RBC

Trust Verification Phase: An AP cross-checks the DBT value of common neighbors of two nodes. If the mismatch in their values is more than the threshold value, it marks the node as suspected. The AP computes each node's indirect BT value (IBT) by aggregating all the BT and estimates the total trust. In the trust verification phase, the AP receives all the TRUST_COLLECTION _REQ from the nodes N_i. It then cross-checks the DBT value of common neighbors of two nodes. If there is a mismatch, it marks the node which has sent the response message as suspected. Otherwise, it computes the indirect BT value (IBT) of each node (by aggregating all the BT values from its neighbors) and estimates the Total Trust (TT). Then AP replies back with a TRUST_COLLECTION_REP message containing the TT values of each node along the reverse path.

Trust Evaluation Phase: The source selects the path with the highest total trust value and shortest Hop Count (HC). The source selects the path with a higher TT value and shorter hop count (HC) in the trust evaluation phase.

The computation of Direct Behavioral Trust is based on the following parameters:

1. Data Forwarding Rate (DFR): "The DFR of a node N_j is the ratio of the number of packets (N_{FWD_j}) forwarded by N_j to the total number of packets received (N_{RCD_j}) by the node N_j" [29]. Data Forwarding rate of a node N_j is given by equation (1).

$$DFR_j = \frac{N_{FWD_j}}{N_{RCD_j}} \quad (1)$$

2. Data Forwarding Time (DFT): The DFT of a node N_j (as given in equation 2) is the ratio of time at which the packet was forwarded by N_j to the time at which the packet was received by N_j.

$$DFT_j = \frac{T_{FWD_j}}{T_{RCD_j}} \quad (2)$$

3. Remaining Battery Capacity (RBC): "The expected remaining battery capacity of a node N_j is computed as the ratio of a battery lifetime (BLT) and battery capacity (BC) of the node" [26]. The expression of the remaining battery capacity is shown in Equation 3.

$$RBC_j = \frac{BLT_j}{BC_j} \quad (3)$$

4. Direct Behavioral Trust (DBT) of a node N_j can be estimated by equation (4):

$$DBT_j = \frac{(w_1.DFR_j)(w_2.RBC_j)}{(w_3.DFT_j)} \quad (4)$$

where w_1, w_2 and w_3 are the weight values of the corresponding metrics such that ($w_1 + w_2 + w_3 \approx 1$).

Various phases of the proposed TCCRP protocol as explained

RESEARCH ARTICLE

in detail with an example as follows:

3.1. Trust Collection Phase

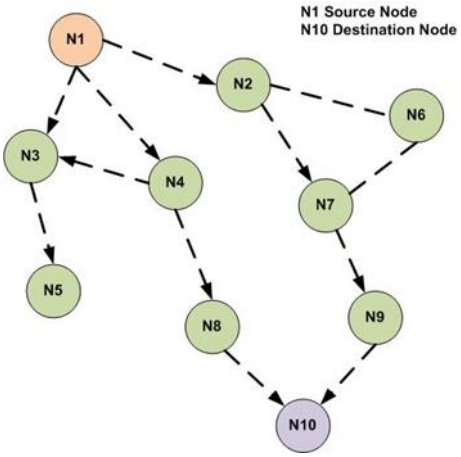
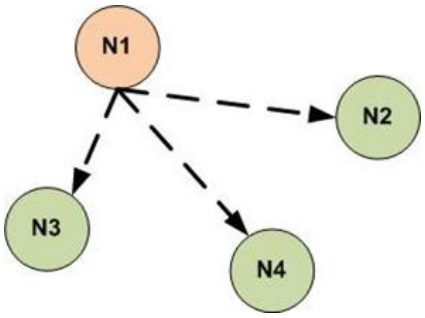
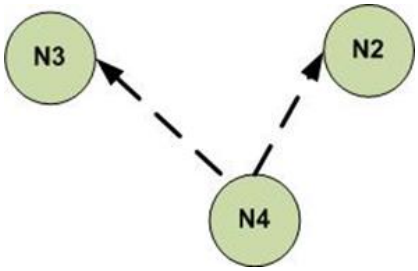


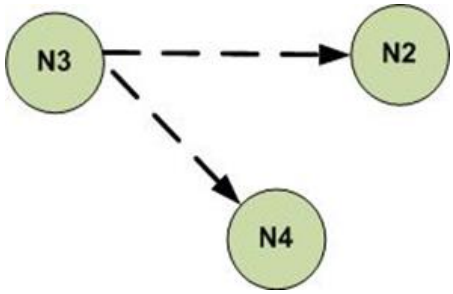
Figure 4 Trust Collection Phase



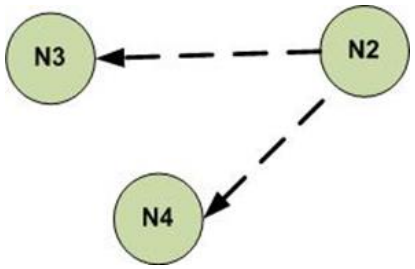
Case I



Case I I



Case III



Case IV

Figure 5 Initialization of Trust Collection Phase

Figure 4 shows the overall trust collection phase of TCCRP, in which the Access Point (AP) broadcasts a TRUST_COLLECTION_REQ (TCR) message to all WSN nodes. The message format is shown in Table 1. On receiving this request, each device N_i estimates the Direct Behavioral Trust (DBT) of its neighbors as described below.

Let N_1 and N_{10} be the source and destination nodes, respectively. Some of the remaining nodes may act as routers. The steps involved in this phase are as follows:

1. The source N_1 floods a TR_COLL_REQ message towards its neighbours N_2, N_3 and N_4 (Figure 5 Case I).
2. On receiving this request, the node N_4 estimates the DBT of its neighbours N_2 and N_3 (Figure 5 Case II). Similarly, N_3 estimates the DBT of N_2 and N_4 (Figure 5 Case III) and N_2 estimates the DBT of N_3 and N_4 (Figure 5 Case IV).
   Let Table 2 show typical DBT values of N_2 and N_3 estimated by N_4. Values of DFR, DFT and RBC (shown in Table 2) are taken as sample values through the simulation process.

Table 2 DBT Values of N_2 and N_3 Estimated by N_4

Node ID	Hop Count	DFR	DFT	RBC	DBT
N_2	1	0.7	0.3	0.8	0.56
N_3	1	0.6	0.5	0.7	0.25

For example, let's assume the values of w_1, w_2 and w_3 as 0.3 each, the value of DBT (shown in Table 2) estimated by node N_4 for node N_2 using the Equation (4) will be as follows:

$$DBT_j = \frac{(0.3 \times 0.7)(0.3 \times 0.8)}{(0.3 \times 0.3)} = 0.56$$

3. Node N_4 then appends the DBT information of its neighboring nodes along with their ID and hop count in the TR_COLL_REQ message and forwards it to N_8. For example, the typical message from node N4 would be TR_COLL_REQ: [N_4(N_2, 1, 0.56), (N_3, 1, 0.25)]

RESEARCH ARTICLE

4. This process is repeated at all the intermediate nodes and finally, all such messages reach N_{10}.

3.2. Trust Verification Phase

In the trust verification phase, the AP (N10) receives all the TR _COLL_REQ from the nodes N(i). It then cross-checks the DBT value of common neighbours of two nodes. If there is a mismatch, it marks the node which sends that request message as suspected. Otherwise, it computes each node's indirect BT value (IBT) and estimates the total trust TT. The complete process is explained in the following flowchart (Figure 6).

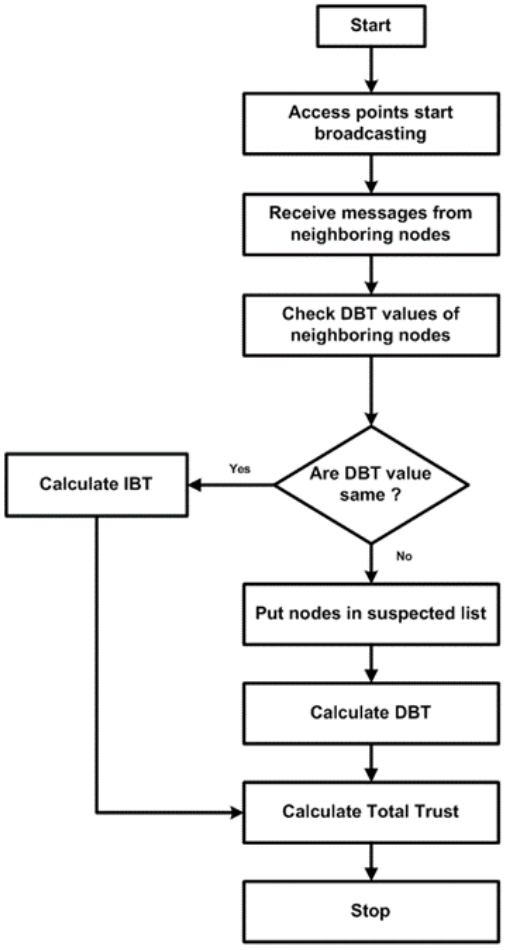


Figure 6 Flowchart for Trust Verification

The steps involved in this process are as follows:

1. The destination node N_{10} receives the TR_COLL_REQ message from the routes $R_1: N_1 - N_4 - N_8$, $R_2: N_1 - N_3 - N_5 - N_8$ and $R_3: N_1 - N_2 - N_7 - N_9$.
2. It then cross-checks the DBT values of common neighbour nodes. For example, the node N_2 is the common neighbour of N_4 and N_7. Hence it appears in the TR_COLL_REQ message of the routes R_1 and R_3. As shown in (Figure 6), the flow chart explains the process of the trust verification phase.
3. If the Direct Behavioural Trust (DBT) value of N_2, along R_1 and R_3 are significantly different, then the nodes N_4 and N_7 are put under the suspected list. It then cross-checks the DBT of these nodes from other nodes list and then eliminates the one having lesser DBT.
4. On the other hand, if there is no mismatch at the common neighbour nodes, it then estimates the Indirect Behavioural Trust (IBT) value by aggregating all the DBT values from its neighbours as per the Equation (5)

$$IBT = \sum DBT_j \quad (5)$$

5. The receiver then estimates the total trust value (TT) of a node N_j as per the following Equation (6)

$$TT_j = \alpha * IBT_j \quad (6)$$

where α is a trust decay factor that decreases as the time stamp expires.

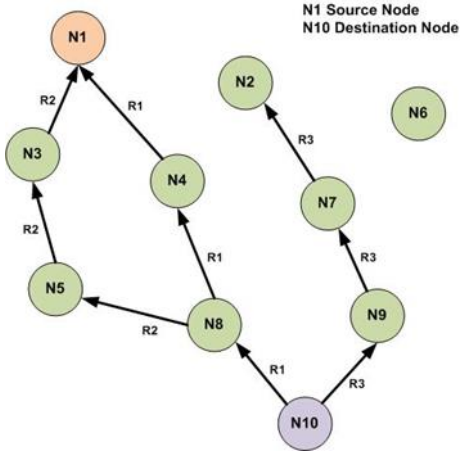


Figure 7 Trust Verification Phase

6. The receiver then generates a trust collection reply message (TR_COLL_REP) containing the TT values of each node along the reverse path $R_1: N_8 - N_4 - N_1$
TR_COLL_REP: [(N_8,1,4.5), (N_4,2,5.20)] Similarly, it transmits the TR_COLL_REP to N_1 through the other reverse paths R_2 and R_3 (as shown in **Figure 7**).

3.3. Trust Evaluation Phase

In this phase, the source selects the more trusted shortest path by checking the node's total trust (TT) values along each path from the TR_COLL_REP. The algorithm of the proposed

RESEARCH ARTICLE

TCCRP protocol is shown in Algorithm 1 of the TCCRP Trust Evaluation algorithm [TCCRP]:

1 R_i← Number of routing paths in networks
⊳i= 1 to 3
2 N_j← Number of nodes in networks
⊳j= 1 to 10
3 PT_i←Trust of path
4 HC_i←Hop count in path
5 TT_j←Total Trust of nodes
6 The source N_1 receives TR_COLL_REP from the paths R_1, R_2 and R_3.
7 For each path R_i, i=1,2,3
8 Do
9 estimate the trust of each path
10 $PT_i = \sum TT_j$
11 estimate the total Hop-count (HC_i) for each R_i
12 if (PT_i = Maximum and HC_i=Minimum) then
13 Select the path R_i for transmission
14 else
15 if (PT_i = Maximum) then
16 Select the path R_i for transmission
17 end if
18 end if

Algorithm 1 TCCRP-Trust Evaluation Method

4. SIMULATION SETUP AND NODE DEPLOYMENT

4.1. Simulation Parameters

Table 3 Simulation Parameters of a WSN for Evaluation of TCCRP

Parameters	Corresponding Values
Number of sensor nodes	100
Size of the Topology	1
MAC Protocol	IEEE 802.15.4
Traffic Type	Constant Bit Rate (CBR)
Numbers of attackers	1,2,3,4,5
Propagation mode	Two ray ground
Battery Energy Assigned	1 Joule
Transmit Power	0.5 Watts
Receive Power	0.3 Watts

Table 3 shows the simulation parameters used as an example for the performance evaluation of the proposed Trust-based Co-operative Cross-layer Routing Protocol (TCCRP) protocol. TCCRP is implemented in the WirelessHART module of NS2. The performance of the proposed protocol is compared with the TMSRS protocol by Fang et al. (2019b) [4] in terms of the metrics packet delivery ratio, throughput, false-positive rate, and residual energy.

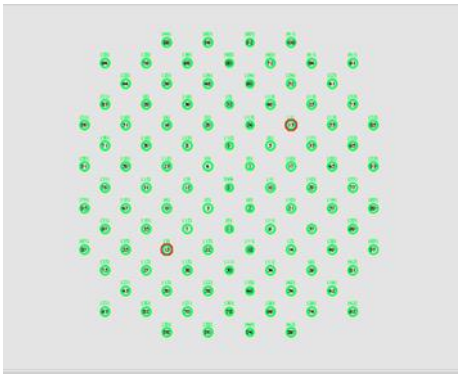


Figure 8 Topology of Proposed Network (100 Sensor Nodes with Two Attacker Nodes)

For the simulation purpose in the proposed TCCRP protocol number of normal nodes is taken as 100. The attacker's sensor node is considered in the range of 1-5. Circled nodes green color nodes in the simulation topology shown in Figure 8 represent the normal nodes, while dark red circled filled up nodes are considered attacker nodes.

5. RESULT AND PERFORMANCE ANALYSIS OF PROPOSED TCCRP PROTOCOL

This section describes the merits of the proposed TCCRP protocol over the existing TMSRS protocol. Simulation has been done in network simulator (ns-2). Various QoS parameters like throughput, packet delivery ratio, false-positive rate, and residual energy are investigated in DDoS attacks and misbehave attacks. Simulations are done by considering the 100 good nodes and five attacker nodes in both DDoS and misbehave attacks scenarios to show the performance of the proposed TCCRP protocol and TMSRS protocol. The proposed TCCRP protocol is based on a cross-layer mechanism where physical and network layers work in collaboration to offer trust-based routing. Packet delivery is done on the basis of minimum hop count. Routing is based on a cross-layer-based trust mechanism that provides better industrial wireless sensor network security. The integrity of information and minimum delay during flow are important constraints. The proposed protocol TCCRP is tested under two different attack conditions: a DDoS attack at the physical layer and misbehave attack at the network layer.

Distributed Denial of services (DDoS) attack harms the multiple functionalities in wireless sensor networks. These

RESEARCH ARTICLE

multiple functionalities especially include the power functioning of sensor nodes where the attacker tries to waste the power of nodes through the denial of services. If multiple attackers attack the wireless sensor network, then it is called distributed attack. In the performance analysis of the proposed protocol, the reduction in residual energy of nodes is taken into consideration, along with the throughput and packet delivery ratio.

Misbehave attack is another threat to the security of a wireless sensor network. An attacker tries to change the normally configured functionalities of any nodes, resulting in the abnormality in terms of desired functions treated as misbehaving. If this misbehave is not detected at the proper time, it results in the improper utilization of resources offered to that wireless sensor network.

Performance analysis of the proposed TCCRP protocol is done on the following QoS parameters:

5.1. Throughput

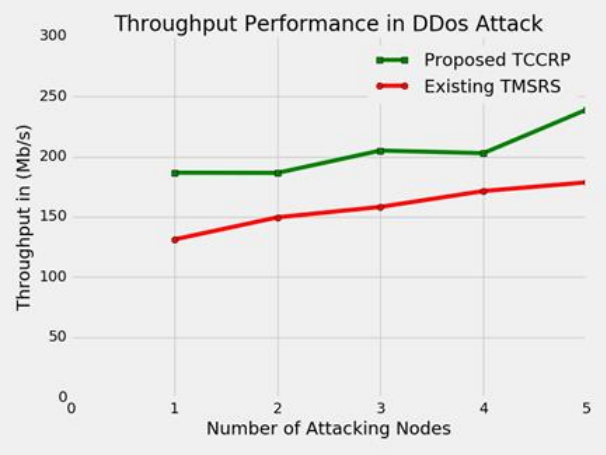


Figure 9 Throughput Performance Under DDoS Attack

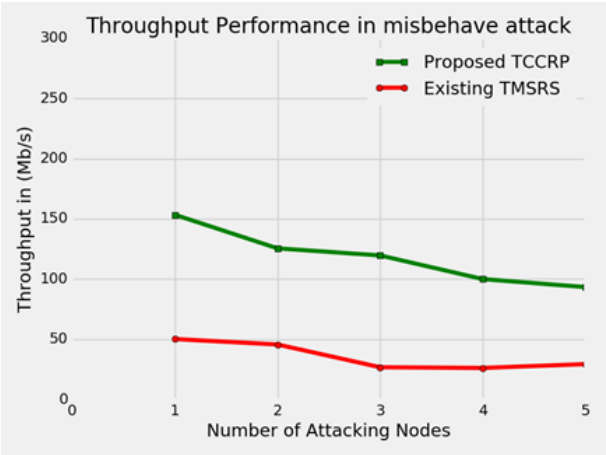


Figure 10 Throughput Performance Under Misbehave Attack

Throughput is an important QoS parameter measured as the number of packets received by a receiving node per second for a network. The higher the number of packets per second higher will the value of network throughput. Throughput parameter is generally influenced by attacking nodes. If the attacking nodes start to increase, they may try to reduce the throughput. As shown in the graph, especially in DDoS case and in the presence of only a single attacker node (as shown in Figure 9), the value of throughput is obtained through the proposed TCCRP as 42% higher as compared to the existing TMSRS protocol. There are multiple factors involved in the TCCRP to show the higher throughput. First, due to the shortest path routing, sufficient energy is available in sensor nodes; also, the value of the packet delivery ratio is higher with a minimum false-positive rate. With the increase in the number of attacking nodes, the throughput parameter is decreased slightly by 33% as compared to the TMSRS protocol.

Similarly, in the case of the device misbehaving, we got that a significant amount of throughput is achieved when the number of attacking nodes is 1 or 5 (as shown in Figure 10). A new routing mechanism will start whenever the TCCRP detects any malicious node, and the packet is again routed on the shortest hop count path. Overall in case of a DDoS attack, the proposed TCCRP protocol improves throughput by 22.8% and in case of misbehaving attack by 70%.

5.2. False Positive Rate

All the sensor nodes employed in the IWSN are usually event-driven or event-sensitive nodes. Especially for industrial applications, these events are highly susceptible. Therefore, these IWSN sensor nodes typically respond whenever an event occurs. But sometimes, these sensor nodes act like malicious nodes and behave abruptly under the influences of other attacking nodes or some irregularities inside the node. For example, these nodes start to respond when there is no event. This activity is treated like a false-positive rate.

The proposed TCCRP protocol tries to resolve this issue to a certain extent compared to the existing TMSRS protocol. In the proposed TCCRP protocol, nodes are considered as trusted nodes. Trust is exchanged and verified amongst all the communicating nodes that are part of that application before sensing any event. If the node can exchange the trust, then that node can sense only varied events and try to generate or give the response according to that event. From Figure 11 and Figure 12, it is clear the false positive rate of the proposed TCCRP protocol is very low compared to existing TMSRS. Hence, the proportion of malicious nodes producing unnecessary responses is more diminutive in numbers in the proposed TCCRP. For example, the false-positive rate for 1st attacker in DDoS attack is 69% less as compared the existing TMSRS.

RESEARCH ARTICLE

On the other hand, in case of misbehave attack, the FPR rate is 76% higher as compared to the existing TMSRS. But as the attacking nodes are increased from 1 to 5, then in the case of a DDoS attack, FPR is further increased to 72% and in misbehave attack, it is 68%. This reduction in FPR due to misbehaving attacks is that attacker nodes are increasing, aiming to disturb the normal functionality of sensor nodes. Hence false-positive rate is much more prone to misbehave attack in case of the number of attacking nodes is increased. Overall in the case of DDoS attack, the proposed TCCRP protocol shows an improvement in FPR by 74% and in the case of misbehaving attacks by 68%.

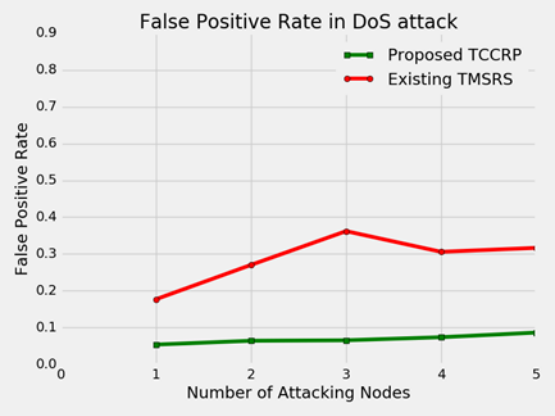


Figure 11 False Positive Rate in DDoS Attack

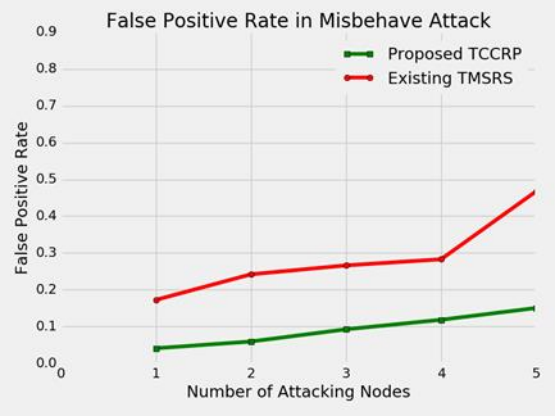


Figure 12 False Positive Rate in Misbehave Attack

5.3. Residual Energy

Residual energy is the remaining battery energy left of a sensor node at a given time. It is energy left at a node after all the inside working mechanisms in sensor nodes such as transmission/reception, communication, computation, sensing, etc. For sending each packet sensor node requires a certain amount of energy. The proposed TCCRP protocol is designed to work on the basis of minimum hop count, and TCCRP will forward the packets where it gets information regarding the shortest routes. TCCRP maintains the list of routes of the shortest path. Due to the shortest path forwarding the packet from one node to another node, minimum energy will be consumed overall.

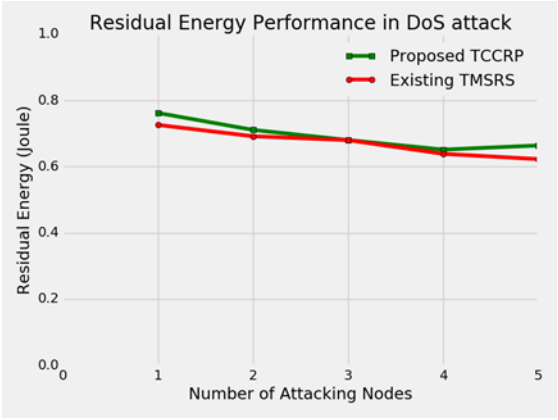


Figure 13 Residual Energy in DDoS Attack

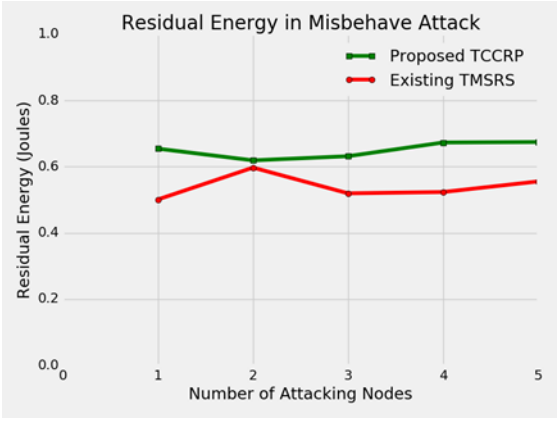


Figure 14 Residual Energy in Misbehave Attack

Figure 13 and Figure 14 show the residual energy in the case of DDoS and misbehaving attacking modes, respectively. In such a scenario, the proposed protocol TCCRP outperforms as compared to the existing TMSRS protocol. In TCCRP initially, the energy consumption is very low, which is the situation before trust exchange. But once the trust verifications and exchange process begin, normal sensor nodes start communicating with each other, which results in an increase in energy consumption during the data transmission phase. In DDoS and misbehave attacks, energy consumption further increases once attacking nodes start attacking. However, the packets are transmitted/received on the basis of trust exchange and verification. Moreover, routing is followed on the basis of the shortest path mechanism. Hence due to trust verifications amongst the normal nodes and the shortest hop-count routing, the energy consumption reduces, resulting in the enhancement in the residual energy and overall lifetime of sensor networks.

RESEARCH ARTICLE

Initially, in the case of a single attacking node, the residual energy of the proposed TCCRP protocol is 5% more than the existing TMSRS in a DDoS attack; similarly, in misbehave attack percentage saving of the proposed TCCRP in residual energy is 30% higher as compared to TMSRS. As the number of attacking nodes increases from 1 to 5, the percentage saving in residual energy through proposed TCCRP is achieved in DDoS attack is 7%, while in misbehave attack saving is 21%. So it's clear that a DDoS attack, due to the distributed nature where all the nodes will try to attack simultaneously, results in a limited amount of residual energy saving, while in misbehave attack, a significant amount of energy is being saved. Overall, in the DDoS attack, the proposed TCCRP protocol shows an improvement in residual energy by 3% and in the case of misbehaving attacks by 19%.

5.4. Packet Delivery Ratio

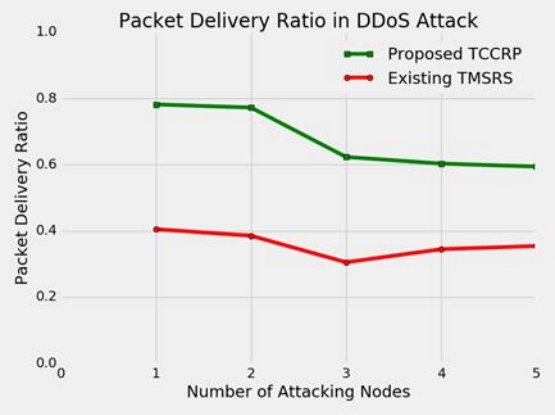


Figure 15 Packet Delivery Ratio in DdoS

The ratio of the total number of packets received at the destination to the total number of packets generated by sources is called the Packet Delivery Ratio (PDR). It is one of the important QoS parameters. Figure 15 shows the performance analysis of the proposed TCCRP protocol under the DDoS, and its comparison is made with the existing TMSRS protocol. Since the PDR is mainly affected in DDoS cases, simulation has been done only for DDoS attacks. During the single node DDoS attack, the packet delivery ratio of the proposed TCCRP is 93% higher than exiting TMSRS, but as the number of attacking nodes increases in number, e.g., five, the PDR is 68% higher than existing TMSRS. TCCRP is based on trust exchange between the valid normal sensor nodes. In TCCRP, typically, packets are exchanged (transmitted and delivered) between the two trusted nodes, but as the number of attacking nodes increases in networks, the PDR performance of TCCRP protocol degrades. However, improved performance is better compared to the existing TMSRS protocol. Overall in the case of DDoS attacks, the proposed TCCRP protocol shows an improvement in packet delivery by 46%.

6. CONCLUSION

A trust-based cooperative cross-layer routing protocol (TCCRP) for IWSN is proposed in this paper. The proposal is based on cross-layer design architecture using physical and network layer parameters to find the trusted routes among the available alternatives. The proposed cross-layer trust-based routing is based on selecting the path with the highest total trust value and shortest hop count. Furthermore, QoS parameters for wireless sensor networks like throughput, false-positive rates, residual energy, and packet delivery ratio are considered. The reason for choosing the trust-based protocol is that the cryptography process has certain limitations in detecting the misbehave attack/node. Another advantage of using the trust-based protocol is that it consumes less power than cryptography processes; hence, the trust-based method increases the lifetime of a wireless sensor network. The simulation results show that the performance of the proposed TCCRP protocols is improved in terms of higher throughput, packet delivery ratio, and residual energy with a lesser false positive rate as with TMSRS in DDoS and Misbehave attacks. In the case of a DDoS attack, the proposed protocol has improved throughput by 22.8%, Packet delivery ratio by 46%, residual energy by 3%, and reduction in false-positive rate by 74%. On the other hand, in case of misbehave attack, the proposed protocol shows a performance improvement in throughput by 70%, residual energy by 19%, and a reduction in false-positive rate by 68%. Therefore it is concluded that the proposed TCCRP has better overall performance than the TMSRS protocol.

REFERENCES

[1] M. Majid, “Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review,” Sensors, vol. 22, no. 6, p. 2087, Jan. 2022, doi: 10.3390/s22062087.

[2] M. Perisa, T. M. Kuljanic, I. Cvitic, and P. Kolarovszki, “Conceptual model for informing user with innovative smart wearable device in industry 4.0,” Wireless Networks, vol. 27, no. 3, pp. 1615–1626, Apr. 2021, doi: 10.1007/s11276-019-02057-9.

[3] P. M. Kumar, G. C. Babu, A. Selvaraj, M. Raza, A. K. Luhach, and V. G. Díaz, “Multi-criteria-based approach for job scheduling in industry 4.0 in smart cities using fuzzy logic,” Soft Computing, vol. 25, no. 18, pp. 12059–12074, Sep. 2021, doi: 10.1007/s00500-021-05765-7.

[4] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, “TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing,” Wireless Networks, vol. 26, no. 5, pp. 3169–3182, 2019.

[5] S. Yu and J. He, “Providing trusted data for industrial wireless sensor networks,” EURASIP Journal on Wireless Communications and Networking, vol. 2018, no. 1, p. 289, Dec. 2018, doi: 10.1186/s13638-018-1307-y.

[6] M. Bal, “An industrial Wireless Sensor Networks framework for production monitoring,” 2014 IEEE 23rd International Symposium on Industrial Electronics (ISIE), pp. 1442-1447. IEEE, 2014, doi: 10.1109/ISIE.2014.6864826.

[7] L. Liu, G. Han, Y. He, and J. Jiang, “Fault-tolerant event region detection on trajectory pattern extraction for industrial wireless sensor networks,” IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2072–2080, 2019.

RESEARCH ARTICLE

[8] L. B. Hormann, C. Kastl, H.-P. Bernhard, P. Priller, and A. Springer, "Lifetime security concept for industrial wireless sensor networks," in 2020 16th IEEE International Conference on Factory Communication Systems (WFCS), pp. 1–8, 2020.
[9] L. Li, "A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2091–2101, 2019.
[10] A. Tiab and L. Bouallouche-Medjkoune, "Routing in Industrial Wireless Sensor Networks: A Survey." Chinese Journal of Engineering, p.7, Feb. 2014. doi: 10.1155/2014/579874.
[11] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2014, pp. 1–14, Jan. 2014, doi: 10.1155/2014/209436.
[12] Z. Teng, C. Du, M. Li, H. Zhang, and W. Zhu, "A Wormhole Attack Detection Algorithm Integrated With the Node Trust Optimization Model in WSNs," IEEE Sensors Journal, vol. 22, no. 7, pp. 7361–7370, Apr. 2022, doi: 10.1109/JSEN.2022.3152841.
[13] B. Mbarek, M. Ge, and T. Pitner, "An adaptive anti-jamming system in HyperLedger-based wireless sensor networks," Wireless Networks, vol. 28, no. 2, pp. 691–703, Feb. 2022, doi: 10.1007/s11276-022-02886-1.
[14] Y. Lai, "Identifying malicious nodes in wireless sensor networks based on correlation detection," Computers & Security, vol. 113, p. 102540, Feb. 2022, doi: 10.1016/j.cose.2021.102540.
[15] Y. Han, H. Hu, and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm," IEEE Access, vol. 10, pp. 11538–11550, 2022, doi: 10.1109/ACCESS.2022.3144015.
[16] T. Khan, "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs," Future Generation Computer Systems, vol. 125, pp. 921–943, Dec. 2021, doi: 10.1016/j.future.2021.06.049.
[17] M. Mathapati, T. S. Kumaran, A. Muruganandham, and M. Mathivanan, "Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 6047–6055, Jun. 2021, doi: 10.1007/s12652-020-02169-7.
[18] I. Ahmad, "Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks," Wireless Communications and Mobile Computing, vol. 2021, p. e1444024, Dec. 2021, doi: 10.1155/2021/1444024.
[19] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collecting in smart city," IEEE Transactions on Industrial Informatics, 2020.
[20] M. S. Sumalatha and V. Nandalal, "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, pp. 1–15, 2020.
[21] C. Liu and X. Li, "Fast, Resource-Saving, and Anti-Collaborative Attack Trust Computing Scheme Based on Cross-Validation for Clustered Wireless Sensor Networks," Sensors, vol. 20, no. 6, p. 1592, Jan. 2020, doi: 10.3390/s20061592.
[22] M. Raza, S. Hussain, H. Le-Minh, and N. Aslam, "Novel MAC layer proposal for URLLC in industrial wireless sensor networks," ZTE Communications, vol. 15, no. S1, pp. 50–59, 2020.
[23] K. P. Uvarajan and C. Gowri Shankar, "An Integrated Trust Assisted Energy Efficient Greedy Data Aggregation for Wireless Sensor Networks," Wireless Personal Communications, pp. 1–21, 2020.
[24] Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, "A trust-based minimum cost and quality aware data collection scheme in P2P network," Peer-to-Peer Networking and Applications, pp. 1–24, 2020.
[25] M. Elsharief, M. A. A. El-Gawad, H. Ko, and S. Pack, "EERS: Energy-Efficient Reference Node Selection Algorithm for Synchronization in Industrial Wireless Sensor Networks," Sensors, vol. 20, no. 15, p. 4095, 2020.
[26] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, "LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system," Journal of Computer Networks and Communications, vol. 2019, 2019.
[27] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TME 2 R: Trust Management-Based Energy Efficient Routing Scheme in Fog-Assisted Industrial Wireless Sensor Network," in International Conference on 5G for Future Wireless Networks, 2019, pp. 155–173.
[28] T. Yang, X. Xiangyang, L. Peng, L. Tonghui, and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," Procedia Computer Science, vol. 131, pp. 1156–1163, 2018, doi: 10.1016/j.procs.2018.04.289
[29] Chinnaswamy S, K A. Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks. Computers and Electrical Engineering 91: pp. 107-130, 2021.

Authors

Manish Panchal is pursuing a Ph.D. from the Department of Electronics and Telecommunication of the Institute of Engineering and Technology (IET) DAVV Indore. He received his Master's degree in Telecommunication System Engineering and a Bachelor of Engineering degree from the Department of Electronics and Telecommunication Engineering SGSITS Indore (1998-2001), India. Currently, his research focuses on the area of computer networks and wireless sensor networks.

Raksha Upadhyay received her Ph.D. from Devi Ahilya University, Indore, India, in 2014. Before joining Devi Ahilya University, she worked as an assistant professor at Shri G. S. Institute of Technology & Science, Indore, India. She is currently an Associate Professor at the Institute of Engineering & Technology at Devi Ahilya University. She has over 20 years of experience in teaching and has published over 30 papers related to wireless communication in reputed journals and conferences. Her research interests include physical layer security, fiber wireless access networks, network performance evolution, and wireless communication networks.

Prakash D. Vyavahare (SM-IEEE (USA), F-IETE (India), F-IE (India)) is a former Professor in the Department of Electronics and Telecommunication Engg. at S. G. S. Institute of Technology and Science, Indore, India. He received his M. Tech. and Ph. D. degrees from IIT Bombay in 1976 and 1995. He worked at Tata Institute of Fundamental Research, Bombay as a Communication Engineer from 1976 to 1982. He was a Hindu-Hitachi scholar at Hitachi Ltd. Japan from 1981-82. He then joined SGSITS Indore (1982) and in the past, held various positions in the institute, such as Head of the Department, Dean (R & D) and Dean (Administration). He retired from SGSITS in the year 2018. He was an associate of ICTP (UNESCO organization), Trieste, Italy from 1998 to 2005. He has 30 papers to his credit in international and national journals including IEEE Transactions in Communications, IEEE Transactions on Electronic Devices and IEEE Transactions on Instrumentation and Measurement. He has guided eight Ph. D. students and three scholars are pursuing their research under his supervision. In the past, he has delivered seminars at various conferences and organizations including CERN (Geneva) Switzerland, Milan polytechnic Milan, Italy and INRIA Rocquencourt France. His areas of interest include channel coding, channel modeling, cross-layer design issues and secure communication.

RESEARCH ARTICLE

How to cite this article:

Manish Panchal, Raksha Upadhyay, Prakash Vyavahare, "Trust-Based Co-Operative Cross-Layer Routing Protocol for Industrial Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 9(3), PP: 292-304, 2022, DOI: 10.22247/ijcna/2022/212555.