Abstract

Objectives: Due to restricted computational power and energy resources, aggregation of data from multiple Sensor Nodes (SNs) secure routing is a significant problem because of highly susceptible in WSNs (Wireless Sensor Networks). Hence ascertaining trustworthiness of data is vital for WSNs. Group-based Trust Management Scheme (GTMS) introduced the trust that depends on direct and indirect monitoring. However, it consumes more energy to communicate the data transmission in WSNs. The main objective of this paper is to transmit the data through the trust node and secure data transmission in WSNs. Methods: The cluster head plays an important role in the cluster-based network. In this paper, we propose Design of Hierarchical Trust based Efficient Cluster Head Selection in WSN (HTECH) which demonstrates the Cluster Head (CH) selection process based on Trust based routing in WSN. This trust is evaluated based on node cooperative-ness, Unselfishness, honest and data transmission rate. Findings: The trust evaluation is used to avoid the malicious and selfish node present in the routing path. Thus, this method provides a realistic and secure approach to choose a shortest path in all trusted path. The simulation results shows that the HTECH scheme reduce both packet loss rate, delay, and improve the throughput in WSNs. Improvements: The HTECH trust routing remove the untrustworthy nodes in order to obtain a reliable passage delivery route also reduce the energy consumption when compared to the existing method.

Keywords: Clustering, Selfishness, Cooperativeness, Trust Routing, WSNs

1. Introduction

Wireless Sensor Networks (WSNs) have been widely applied in various industrial applications, e.g., surveillance operations, an analysis of disease, monitoring of patient and equipment, source detection, fault prediction, pollution monitoring, sea searching, tide monitoring and report collected data to the sink by using multi-hop wireless communications. The nodes able to collaborate and self organize together in order to establish and maintain the network\(^1\). Clustering means grouping of nodes that are close to each other and the main purpose is to reduce the energy consumption and routing overhead\(^2\). However, the wireless and resource-constraint nature of a sensor network creates it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trust worthiness of another node.

Distributed and Safe Weighted Clustering Algorithm\(^3\) detects common routing problems and attacks in clustered WSNs that depend on behavioral level in order to
remove the malicious node. This weighted clustering algorithm detects the internal misbehavior nodes during distributed monitoring process. It also decrease energy utilization and guarantees the choice of legitimate CHs. Light Weight Intrusion Detection System\(^9\) integrated for clustered sensor networks uses an over hearing mechanism to reduce the sending alert packets. This approach focuses around strategy of distributed resolution enables to generate a reduced number of balanced and homogeneous clusters that reduces the energy utilization of the network and prolongs the sensor lifetime.

Trust management scheme based on behavior feedback\(^2\) was proposed to support forwarding protocols in extremely sparse opportunistic networks. By applying the certificate chains based on social attributes, the mobile nodes build the local certificate graphs gradually to realize the web of Identity Trust relationship. Trust management scheme can efficiently explore and filter the trust nodes for secure forwarding in opportunistic networks. Hierarchical trust management protocol\(^6\) applies both trust-based intrusion detection and trust-based geographic routing. This trust management protocol handles a large number of heterogeneous SNs for scalability and re-configurability. In addition it also deals with selfish or malicious SNs for survivability and intrusion tolerance. It detects the intrusion through optimal trust threshold for minimizing false positives and false negatives. Location verification and trust management for resilient geographic routing\(^7\) proposed trust management protocols and applied them to geographic routing in WSNs. However, no hierarchical trust management was considered for handling clustered WSNs. The work-evaluated trust based on QoS aspects such as packet dropping and the degree of cooperativeness, while it considers both QoS and social trust for trust evaluation of a SN.

Trust-based intrusion detection in wireless sensor networks\(^8\) contains 3 level trusts such as trust aggregation accuracy, dynamic trust management and application-level trust optimization. Trust aggregation protocol accuracy identifies and validates the best trust aggregation and propagation protocol setting for each individual trust property. Dynamic trust management specifically identifies and validates the best way to form trust out of QoS and social trust properties dynamically in response to changing conditions such as increasing hostility to maximize application performance. Application-level trust optimization identifies the best way to use trust for application performance optimization.

A trust model using fuzzy logic\(^9\), proposed trust model using fuzzy logic for secure communication in the network. The fuzzy logic consist of 3 steps, such as Fuzzy matching, Interference and Combination. This algorithm chooses the proper path from source to destination. Trust based onion routing enhances anonymity protection by constructing onion circuits using trust-based routers. This model isolates the anonymity compromised by interference attacks. Fuzzy Trusted Dynamic Source Routing (FTDSR)\(^10\) protocol evaluated the efficiency of the protocol in malicious node identification and attack resistance. This protocol was divided into two parts that is subjective trust evaluation model and trusted routing model. Subjective trust evaluation model evaluates the nodes behavior. The Analytic Hierarchy Process (AHP) makes the decision on the trust influencing attributes and considering logic rules prediction. FTDSR provides flexible and feasible approach to choose a better path with trust constraint. Secure trust based dynamic source routing\(^11\) evaluates the trust level of its neighbors. This scheme was based on previous experiences, knowledge and recommendations of other neighbors to appraise the trust level of other nodes. It provides a flexible and feasible approach to choose a shortest path in all trusted path. These model nodes interact only with its neighbors. Thus, nodes do not keep trust information about every node in the network.

Trusted and Secure Clustering\(^12\) analyses the impact of signal-strength attacks in cluster communication on trust degree and level of security. This scheme monitors a node to become compromised and presents the signal attenuation impact on cluster communication as a part of extended security consideration. Trusted cluster formation provides trust worthy, energy efficient secure communication in the network. Reputation and Trust concept can be used to overcome the compromised node detection and secure data aggregation problems in WSN. Fast zone-based node compromise detection and revocation\(^13\) framework detects the compromised node in WSN and apply software attestation for the detected compromised nodes that cannot be performed due to a high risk of false positive rate. Secured Anonymous Routing with Digital Signature (SARDS)\(^14\) performs verification of the routing information exchanged among the SNs in WSN.
SARDS apply Elliptical Curve Cryptography (ECC) as the backbone of security formulations and performs authentication of all the communicating nodes present in the network. Cluster Arrangement Energy Efficient Routing Protocol (CAERP)\textsuperscript{15} introduced CH selection algorithm for the data transmission between CHs and the BS. CAERP is an un-even clustering mechanism and it eliminates the initial dead node problem. This algorithm improves Energy efficiency, Network lifetime and Load balancing in WSNs. Group-based Trust Management Scheme (GTMS)\textsuperscript{16} introduced the trust that depends on direct and indirect monitoring. A distributed trust management scheme collects recommendations from all its group members to compute the trust. A centralized trust management approach as each CH collects recommendations of other CHs directly from the sink. GTMS reduces the memory consumption however it consumes more energy to communicate with the sink.

\section*{2. Proposed Method}

\subsection*{2.1 Design of Hierarchical Trust}

Trusted routing can kick out the untrustworthy nodes in order to obtain reliable passagedelivery route. Hierarchical Trust Design process considers four components such as node unselfishness, Node Cooperativeness, Node Honest and Node Data Transmission Rate. Figure 1 describes the diagram of the proposed scheme.

\subsection*{2.1.1 Node Unselfishness Rate}

Node unselfishness refers to the rate of unselfishness. A node may become a selfish to save energy. A selfish node may stop reading data and drops packets it receives. An unselfish node may turn selfish in every trust evaluation interval according to its residual energy and the number of unselfish neighbors around. The node Unselfishness Rate evaluation is given below.

\begin{equation}
N_{USR} = \frac{E_{utilization}}{E_{IE}} + \frac{US_{neighbor}}{N_{degree}}
\end{equation}

$E_{utilization}$ → Energy Utilization

$US_{neighbor}$ → Unselfish Neighbor

$E_{IE}$ → Initial Energy

$N_{degree}$ → Node Degree

![Figure 1. Illustration of proposed scheme.](image-url)
2.1.2 Node Cooperativeness Rate

Node cooperativeness refers to the experience of interaction between neighbor nodes. The Node Cooperativeness is calculated depending upon the difference between the number of Route Request (RREQ) messages to a particular node and the number of non Route Reply (RREP) message to the RREQ message received. The node cooperativeness calculation is given below.

\[ N_{CR} = \frac{RREQ_e - NRREP_e}{RREQ_e} \]  

(2)

\( RREQ_e \rightarrow \)Route Request Count

\( NRREP_e \rightarrow \)Non-Route Reply Count

2.1.3 Node Honest Rate

A compromised node is that which performs some functions different from legitimate node. Every node estimates by keeping a count of suspicious dishonest experience of node based on high discrepancy in the sensor reading, retransmission, repetition and delay. The Node Honest Rate Computation is given below.

\[ N_{HR} = \frac{N_{CN}}{N_{UCN}} \]  

(3)

\( N_{CN} \rightarrow \)Node Compromised Neighbor

\( N_{UCN} \rightarrow \)Node Uncompromised Neighbor

2.1.4 Node Data Transmission Rate

Every node compute the Data Transmission Rate based on the packet sent during time interval. The Node Transmission Rate computation is given below.

\[ N_{DTR} = \frac{\text{Packet sent Rate}}{\text{time}} \]  

(4)

![Figure 2. Working flow of proposed scheme.](image-url)
The Trust Value of every node computation is given below.

\[ T_N = \frac{1}{4}(N_{CR} + N_{USR} + N_{HR} + N_{DTR}) \]  \hspace{1cm} (5)

2.2 Efficient Cluster Head Selection

Hierarchical Trust based Efficient Cluster Head Selection in WSN (HTECH) is designed in which the Base Station (BS) is placed at the corner of the field and SNs forms clusters. Cluster contains SNs and CH. CH is responsible only for receiving data from the CMs, perform aggregation process over the received data and then send to the BS. The CH operations are transmitting, receiving and overhearing. In case the CH is wicked, all process will fail. Therefore, the selecting CH becomes an important task. CH is selected based on the Trust Evaluation. If the trust value is greater than average trust, that node is selected as a CH. CH receives the data from SNs, then aggregates the data and sends it to the BS.

Figure 2 shows the working flow of the proposed scheme in which CH is selected based on the SN Trust. The trust value computation depends on Node Unselfishness Rate, Node Cooperativeness Rate, Node Cooperativeness Rate and Node Data Transmission Rate. If the trust value is greater than the Average Trust then that node is selected as a CH. CH receives the data from SNs, then aggregate these data and send it to the BS.

3. Simulation Analysis

The performance of the HTECH is analyzed by using the Network Simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete event time driven simulator that is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The parameters used for the simulation of the HTECH scheme are tabulated in Table 1. The simulation of the proposed scheme has 50 nodes deployed in the simulation area 1000×600. The nodes are communicated with each other by using the communication protocol User Datagram Protocol (UDP). The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two-ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance

| Parameter               | Value |  |
|-------------------------|-------|---|
| Channel Type            | Wireless Channel |   |
| Simulation Time         | 50 ms |  |
| Number of nodes         | 50    |  |
| MAC type                | 802.11|  |
| Traffic model           | CBR   |  |
| Simulation Area         | 1000×600 |  |
| Transmission range      | 250m  |  |
| Network Interface Type  | WirelessPhy |  |
of the proposed scheme is evaluated by the parameters packet delivery rate, packet loss rate, average delay, throughput and residual energy.

### 3.1 Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. The PDR is calculated by Equation 6.

$$PDR = \frac{\text{Total Packets Received}}{\text{Total Packets Send}}$$  \hspace{1cm} (6)

The Figure 3 indicates the PDR of the proposed scheme HTECH is higher than the PDR of the existing method GTMS. The greater value of PDR means the better performance of the protocol.

### 3.2 Packet Loss Rate

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The formula used to calculate the PLR is given in Equation 7.

$$PLR = \frac{\text{Total Packets Dropped}}{\text{Total Packets Send}}$$  \hspace{1cm} (7)

The PLR of the proposed scheme HTECH is lower than the existing scheme GTMS in Figure 4. Lower the PLR indicates the higher performance of the network.

### 3.3 Average Delay

The average delay is defined as the time difference between the current packets received and the previous packet received. It is measured by Equation 8.

$$\text{Delay} = \frac{\sum_{n=0}^{n} \text{Pkt Send Time} - \text{Pkt Recvd Time}}{\text{Time}}$$  \hspace{1cm} (8)

The average delay for the proposed HTECH scheme is lower than the existing GTMS scheme as shown in Figure 5. Lower delay indicates the better performance of the network.

---

**Figure 3.** Packet delivery rate.

**Figure 4.** Packets loss rate.

**Figure 5.** Average delay.
Figure 5 demonstrates that the delay value is low for the proposed scheme HTECH than the existing scheme GTMS. The minimum value of delay means that higher value of the throughput of the network.

3.4 Throughput

Throughput is the average of successful messages delivered to the destination. The average throughput is calculated using Equation 9.

\[
\text{Throughput} = \frac{\sum_{n} \text{Pkt\:Received}(n) \times \text{Pkt\:Size}}{1000}
\]  

(9)

Figure 6 proves that the proposed scheme HTECH has greater average throughput when compared to the existing scheme GTMS.

3.5 Residual Energy

The amount of energy remaining in a node at the current instance of time is called as residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations.

Figure 7 shows that the residual energy of the network is better for the proposed scheme HTD-ECH when compared with the existing scheme GTMS.

4. Conclusion

The proposed trust-based routing protocol performs close to the ideal performance of routing in delivery rate and decrease the delay. The algorithm out performs the existing method in terms of packet loss rate and energy utilization and also improves the network throughput.

5. References

1. Akyildiz IF, Melodia T, Chowdhury KR. A survey on wireless multimedia sensor networks. Computer Networks. 2007; 51(4):921-60.
2. Safa H, Artail H, Tabet D. A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wireless Networks. 2010; 16(4):969-84.
3. Amine D, Nasr-Eddine B, Abdelhamid L. A distributed and safe weighted clustering algorithm for mobile wireless sensor networks. Procedia Computer Science. 2015; 52:641-6.
4. Hai TH, Huh EN, Jo M. A lightweight intrusion detection framework for wireless sensor networks. Wireless Communications and Mobile Computing. 2010; 10(4):559-72.
5. Xi C, Liang S, Jianfeng M, Zhuo MA. A trust management scheme based on behavior feedback for opportunistic networks. Communications, China. 2015; 12(4):117-29.
6. Bao F, Chen IR, Chang M, Cho JH. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE
Transactions on Network and Service Management. 2012; 9(2):169-83.
7. Liu K, Abu-Ghazaleh N, Kang KD. Location verification and trust management for resilient geographic routing. Journal of Parallel Distributed Computing. 2007; 67(2):215–28.
8. Bao F, Chen IR, Chang M, Cho JH. Trust-based intrusion detection in wireless sensor networks. Proceedings of IEEE International Conference on Communications (ICC); Kyoto. 2011. p. 1–6.
9. Kim TK, Seo HS. A trust model using fuzzy logic in wireless sensor network. Proceedings of World Academy of Science, Engineering and Technology; 2008. p. 1051-4.
10. Xia H, Jia Z, Ju L, Zhu Y. Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. IET Wireless Sensor Systems. 2011; 1(4):248-66.
11. Jain YK, Sharma NK. Secure trust based dynamic source routing in MANETs. International Journal of Scientific and Engineering Research. 2012; 3(8):1-7.
12. Gaur M S, Pant B. Impact of Signal-Strength on Trusted and Secure Clustering in Mobile Pervasive Environment. Procedia Computer Science. 2015; 57:178-88.
13. Ho J-W, Wright M, Das SK. Zone Trust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing. IEEE Transactions on Dependable and Secure Computing. 2012; 9(4):494 –11.
14. Roopashree HR, Kanavalli A. SARDS: Secured Anonymous Routing with Digital Signature in wireless sensor network. Indian Journal of Science and Technology. 2016; 9(7):1-12.
15. Vijayan K, Raaza A. A novel cluster arrangement energy efficient routing protocol for wireless sensor networks. Indian Journal of Science and Technology. 2016; 9(2):1-9.
16. Shaikh RA, Jameel H, d’Auriol BJ, Lee H, Lee S, Song Y. Group-based trust management scheme for clustered wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2009; 20(11):1698–12.