VOL. 11, NO. 19, OCTOBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

AN EFFICIENT DATA COLLECTION SCHEME BASED ON TRUST EVALUATION IN LARGE SCALE WIRELESS SENSOR NETWORKS

Ramalingam L.[1] and Audithan S.[2]
[1]Department of Computer Science and Engineering, St. Peter's University, Chennai, Tamil Nadu, India
[2]Department of Computer Science and Engineering, PRIST University, Kumbakonam, India
E-Mail: ramalingamstpeters@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) play an essential role in today's genuine world applications. The effectiveness of WSNs depends on the data collection. However, traditional data collection schemes fail to provide a guaranteed reliable network in terms of traffic and end-to-end connection. To secure the WSNs against adversaries misdirecting the multi-hop routing, we have designed and implemented EDCTE; An Efficient Data Collection based on Trust Evaluation in Large Scale Wireless Sensor Networks. It provides trustworthy and energy efficient route that would effectively diminish the problems of delay, traffic and end-to-end connection. The Data Collector (DC) collects the data packet from the Cluster Head (CH) and delivers it to the Base Station (BS). The strength of the EDCTE algorithm is to build a simple structure, so as to reduce the energy consumption of the CH and to avoid frequent cluster formation. Simulation results demonstrate that EDCTE provides better QoS in terms of energy consumption, throughput, end-to-end delay and lifetime of the network.

Keywords: trust, clustering, data collector, energy, WSN.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of hundreds to thousands of inexpensive wireless nodes with limited computational capacity and energy resources generally deployed in an unattended location. Most effective utilization of WSNs requires minimization of energy consumption through the design of energy efficient network protocols and algorithms to prolong network lifetime. Since sensor nodes are usually low-priced hardware apparatus, they are highly susceptible and often becomes fault. It imperils the reliability of data transmission and degrades the network performance in terms of packet delivery ratio (PDR) [1]. Single intermediate node can break a route; malevolent nodes can frequently break routes. When a route is broken the nodes have to rely on cycles of time-out and route discoveries to reestablish the route. These route discoveries may incur network wide flooding of route requests that use a significant amount of the network's resources. Breaking the routes increases the delay of packet delivery cause network partitioning and the multi-hop communication to fail. Thus, in order to establish stable routes and maintain continuous traffic flow, it is important to assess the nodes' competence and reliability in relaying packets to make informed routing decisions.

In WSNs, trust management is important to evaluate the nodes trustworthiness, capability and reliability in relaying packets [2]. A node's trust value is defined as the degree of belief about the node's behavior that is the probability that the node will behave as predictable. The trust values are calculated based on past behaviors and are used to predict their future behavior [3]. The majority of the existing trust systems in multi hop wireless networks computes a single trust value for every node. However, a single measure may not be significantly enough to sufficiently depict a node's trustworthiness and capability.

We develop An Efficient Data Collection Scheme based on trust evaluation in Large Scale WSNs. Our goal is to establish the reliable path and improve the network throughput based on trust evaluation. In this scheme, the nodes are grouped into clusters and a node with strong computing power and trusted node is elected as a CH. Establishing trust in a clustered environment provides numerous advantages such as to detect faulty or malevolent within a cluster.

The remainder of this paper is structured as follows. In Section 2, related work is discussed. Section 3 explains the proposed scheme. Simulation results are presented in section 4. Finally, Section 5 provides the conclusion of our work.

2. RELATED WORK

A distributed Hierarchical Dynamic Trust Management Protocol (HTMP) [4] that contains two trust values that is social trust and QoS (Quality of Service) trust. A probability model to examine protocol performance and declared subjective trust against the objective trust obtained based on truth node status. However, implementing a complex trust evaluation at each CM of the cluster is unrealistic. An Energy efficient Reliable Trust-based Data Aggregation protocol (ERTDA) [5] monitors and evaluates the trust values of the nodes and it detects and excludes the compromised nodes in a timely manner. The ERTDA protocol can effectively improve the accuracy of the aggregation, reduce both the node death rate and node energy consumption, improve the reliability of the data communication and lengthen the life of the networks.

Energy-efficient Trust based data Aggregation (ETA) [6] achieves reliable and energy-efficient data transmission and aggregation. ETA uses the concept of functional reputation and trust as a means to reach reliability. Efficient reputation is used to select nodes that

best satisfy the criteria to be collector on the basis of the quality of the node.

Trust-based CH Election Mechanism (TCHEM) [7] can decrease the likelihood of malevolent or compromised nodes from becoming CHs. It does not encourage sharing of trust information among sensor nodes. Therefore, this mechanism reduces the effect of bad mouthing attacks. However, TCHEM does not cover trust in detail, due to numerous key issues of trust management.

Agent-based Trust and Reputation Management (ATRM) [8] introduced a trust and reputation local management strategy with the aid of the mobile agent's management on each node. The advantage of a local management scheme for trust and reputation is that centralized repositories are not required and the nodes themselves are capable of providing their own reputation information whenever requested. Therefore, reputation and propagation is performed without network-wide flooding and with no acquisition-latency. However, ATRM assumes that mobile agents are resilient against malevolent nodes that try to steal or modify information. In several applications, this statement may be improbable.

Feedback Based Secure Routing protocol (FBSR) [9] is resilient against wormhole and Sybil attacks. However, the FBSR create overhead. The trust management mechanism [10] is based on the subjective reputation of comprehensive information as an input and quantifies the results of the trust value as an output.

Trust Aware Geographical Routing scheme (TAGR) [11] relies on both direct and indirect observations to derive the trustworthiness of each adjacent node while it is capable of defending against routing attacks. This scheme reduces the routing overhead and resists some common attacks. However, this trust aware scheme depends on the specific routing scheme that limits the scope of applications.

Trust Aware Routing Protocol (TARP) [12] was proposed to find a trusted adjacent node. The source node will send an adjacent request to all its adjacent asking them for their trust attributes. Once it receives the trust attributes, the source node will choose the most trusted node. Then the source node make a credit check on the pre-selection node by communicating directly with its adjacent node. The source node uses a different channel using higher energy. Frequency-hopping and time synchronization technologies are needed to implement this approach. These complex MAC scheduling mechanisms limit the applications making it unattractive to WSNs.

Establishing STAble and Reliable routes (E-STAR) combines payment and trust systems. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' capability and consistency in relaying packets. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. In this protocol, highly-trusted nodes having sufficient energy to minimize the possibility of breaking the route. E-STAR can get better packet delivery ratio and route stability.

2.1 AN efficient data collection based on trust evaluation in large scale WSNs

The trust mechanism can be used to ensure security in data collection and data forwarding in WSNs. It can be used to detect the compromised and malevolent node to provide the trust relationship between nodes. In this paper, we propose An Efficient Data Collection based on Trust Evaluation (EDCTE) in Large Scale WSNS to improve the reliability of data aggregation and energy efficiency. The EDCTE scheme consists of set-up phase and steady state phase. In the set-up phase, cluster formation, CH and DC selection identifies the optimal path between CMs and BS. Then, the steady state phase is initiated to transfer the data from the CMs to the BS. Figure-1 shows the structure of the EDCTE scheme.

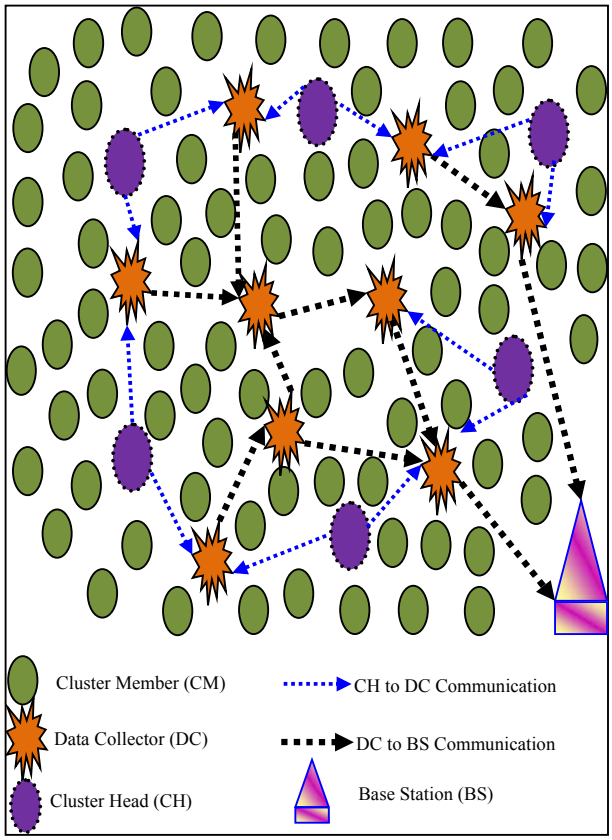

Figure-1. EDCTE structure.

2.2 Setupphase

This phase consist of CH election and DC selection. Every CH needs enough energy for both the data gathering from CMs and forward the data to DC. Thus, the CMs elect the CH based on trust and residual energy. The trust value is determined according to the node behavior. The CH trust values are computed in the equation below.

$$T_{CH} = \frac{S_I}{S_I + US_I} \quad (1)$$

Where

S_I → Total number of Successful interactions

US_I → Unsuccessful interactions

The DC nodes are necessary to select the multiple paths to the BS. While selecting the data transmission path from CH to BS, the BS chooses the DC based on the trust value to ensure selecting the better transmission path. The trust value evaluation according to Feedback Factor (FF) energy and interactions is given below.

The Feedback from the adjacent nodes serves as the dynamic information of the current network; this feedback information is included in the acknowledgement without any usage of extra message for the consideration of avoids network congestion.

$$T_{DC} = \frac{F_F}{S_I + E} \quad (2)$$

Where

F_F → Feedback Factor

E →Energy

The feedback factor F_F is calculated equation is given below.

$$F_F = \frac{P_F + 1}{N_F + P_F} \quad (3)$$

Where

P_F →Positive feedback of Adjacent Node

N_F →Negative feedback of Adjacent Node

2.3 Steady-State Phase

Once the set-up phase is completed, steady-state phase is initiated. In steady-state phase, all the CMs send the collected data to the CH in an allocated time slot. Then, the CH starts to gather and aggregate the data from its CMs. After the DC is initiated to collect the data from its CH, it then forwards the aggregated data packet to the BS. All the CHs are connected with DC and all the DC transmit the aggregated data to the BS. Here, the DC is responsible to collect the data from the corresponding CH and transmit the data to BS.

Figure-2 demonstrate the flowchart of the EDCTE which is a clustering method that uses the DC to collect the data from the CH and deliver it to the BS. Here the BS selects the DC based on the trust and CMs select the CH based on the trust and energy. The CH gathers the data from CMs then aggregate the data. The DC collects the data from the CH and forwards it to the next DC. Once the DC reaches the BS the process is stopped. EDCTE secures the multi-hop routing in WSNs against misdirecting the multi hop routing by evaluating the trustworthiness nodes. EDCTE is also energy efficient, highly scalable and well adaptable.

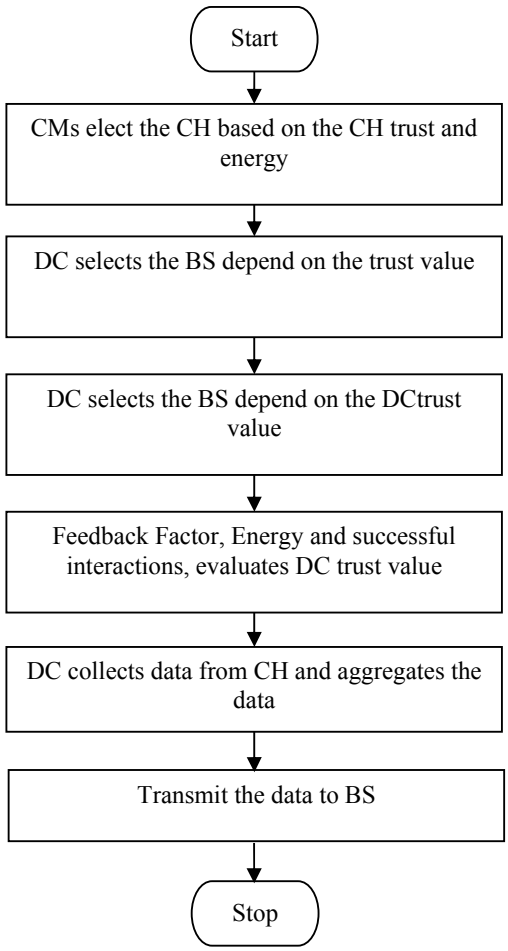

Figure-2. Flow chart of the EDCTE scheme.

3. SIMULATION ANALYSIS

The performance of the EDCTE 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 EDCTE scheme are tabulated in Table-1. The simulation of the proposed scheme has 60 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 of the proposed scheme is evaluated by the parameters packet delivery rate, packet loss rate, average delay, throughput and residual energy.

Table-1. Simulation parameters.

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	50 ms
Number of nodes	60
MAC type	802.11
Traffic model	CBR
Antenna Model	Omni Antenna
Simulation Area	1000×600
Transmission range	250m
Network Interface Type	WirelessPHY

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 (4).

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \quad (4)$$

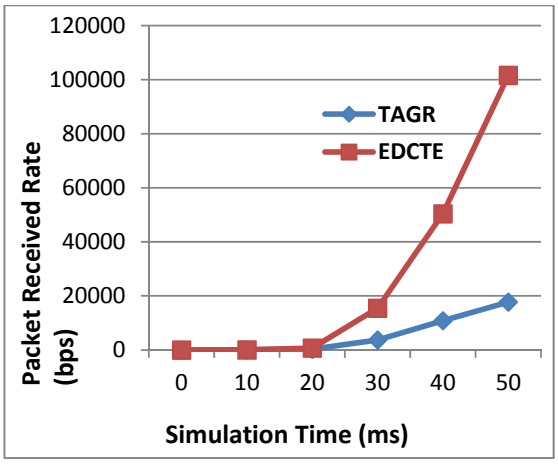

Figure-3. Packet delivery rate.

Observations from Figure-3 indicates that the EDCTE scheme achieve better PDR than the existing method TAGR. The greater value of PDR means the improved 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 PLR is calculated by Equation (5).

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \quad (5)$$

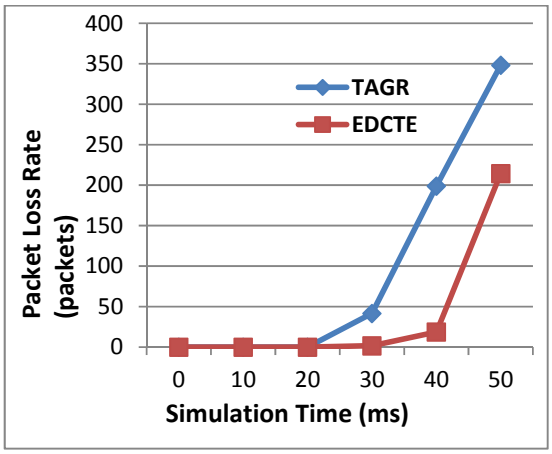

Figure-4. Packet loss rate

The PLR of the proposed scheme EDTCH is lower than the existing scheme TAGR 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 (6).

$$Average\ Delay = \frac{\sum_0^n Pkt\ Recvd\ Time - Pkt\ Sent\ Time}{n} \quad (6)$$

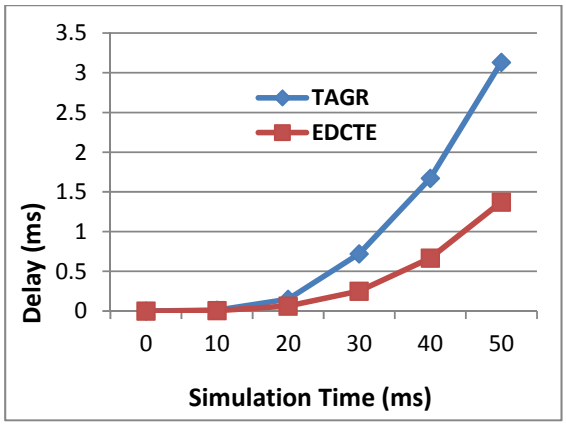

Figure-5. Average delay.

Figure-5 demonstrates that the performance of delay with respect to the simulation time. The result shows that the EDTCH has minimum delay when compared to the existing scheme TAGR. 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 (7).

$$Throughput = \frac{\sum_0^n Pkts\ Received\ (n) * Pkt\ Size}{1000} \quad (7)$$

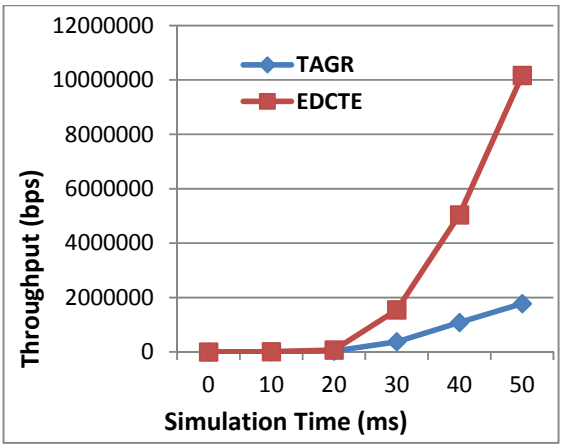

Figure-6. Throughput.

Figure-6 proves that the proposed scheme EDTCH has greater average throughput when compared to the existing scheme TAGR.

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.

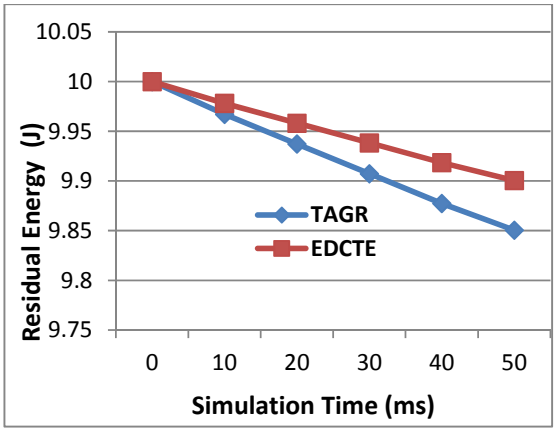

Figure-7. Residual energy.

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

4. CONCLUSIONS

We have designed and implemented EDCTE, An Efficient Data Collection based on Trust Evaluation in Large Scale WSNS to improve the reliability of data aggregation and energy efficiency. EDCTE effectively protects WSNs from severe attacks through trusted routing. With the idea of trust evaluation, EDCTE enables a node to keep track of the trustworthiness of CH and DC thus select a reliable route to minimize the energy utilization, reduces the end-to-end delay and traffic in WSNs. The simulation results prove that the EDCTE provides better throughput, reduces the packet loss rate and improve the network scalability and flexibility.

REFERENCES

[1] Karlof C. and D. Wagner. 2003. Secure routing in wireless sensor networks: attacks and countermeasures. in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications.

[2] Y. Sun, Z. Han, K. J. Ray Liu. 2009. Defense of Trust Management Vulnerabilities in Distributed Networks. IEEE Comm. Mag. 46(2): 112-119.

[3] H. Yu, Z. Shen, C. Miao, C. Leung, D. Niyato. 2010. A Survey of Trust and Reputation Management Systems in Wireless Communications, Proc. IEEE. 98(10): 1752-1754.

[4] Bao F., Chen I. R., Chang M.and Cho J. H. 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. Network and Service Management, IEEE Transactions on. 9(2): 169-183.

[5] Alshehri M. D.and Hussain F. K. 2015, November. A Comparative Analysis of Scalable and Context-Aware Trust Management Approaches for Internet of Things. In Neural Information Processing (pp. 596-605). Springer International Publishing.

[6] Taghikhaki Z., Meratnia N. and Havinga P. J. 2011, April. Energy-efficient trust-based aggregation in wireless sensor networks. In Computer Communications Workshops (INFOCOMWKSHPS), 2011 IEEE Conference on (pp. 584-589). IEEE.

[7] G. V. Crosby, N. Pissinou, J. Gadze. 2006. A framework for trust-based cluster head election in wireless sensor networks, Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems. pp. 10-22.

[8] A. Boukerche, X. Li and K. EL-Khatib. 2007. Trust-Based Security for Wireless Ad Hoc and Sensor Networks, Computer Comm. 30: 2413-2427.

[9] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou. 2008. Fbsr: feedback-based secure routing protocol for

wireless sensor networks. International Journal of Pervasive Computing and Communications.

[10] A. Jsang, R. Ismail and C. Boyd. 2005. A Survey of Trust and Reputation system for online service provision [C]. Decision Support System. pp. 618-644.

[11] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis and P. Karkazis. 2013. A novel trust-aware geographical routing scheme for wireless sensor networks. Wireless Personal Communications. 69(2): 805-826.

[12] L. Abusalah, A. Khokhar, and M. Guizani. 2006. Trust aware routing in mobile ad hoc networks. In Proceedings of the IEEE Telecommunications Conference (GLOBECOM '06). pp. 1-5.

[13] Mahmoud M. M., Lin X. and Shen X. 2015. Secure and reliable routing protocols for heterogeneous multihop wireless networks. Parallel and Distributed Systems, IEEE Transactions on. 26(4): 1140-1153.