Energy Efficient Trust Based Secure Data Transaction in WSN

V.BINDU, Research Scholar,

Vinayaka Mission's Kirupananda Variyar Engineering College, Salem.

Dr.NITHYA.M,

Head of the Department-Computer Science and Engineering,

Vinayaka Mission's Kirupananda Variyar Engineering College, Salem.

ABSTRACT:

Wireless sensor network has been widely utilized everywhere and its application are enhancing day by day. In many research work various approaches has been going on to eradicate its drawbacks to increase network performance. In most of the research work, increasing network life span was focused to attain this energy efficient path allocation algorithms was deployed. However energy loss and methods to reducing it is an emerging research area. In our proposed work, Trust Based Energy Efficient Ad hoc On Demand Distance Vector (T-EEAODV) is used here it construct the path between source to destination considering the parameter such as distance, energy level and trust value of node. By calculating this factor fake node involvement during data transaction is identified and in case if any data loss occurred by pass method is deployed to avoid retransmission of data from source to destination through alternate path. It will consider previous node as source and construct path for efficient data transaction. Hence our proposed work achieves better result compared to existing work and it increases network performance.

I.INTRODUCTION

Wireless sensor network (WSN) is one of the emerging technologies, which finds application in a variety of fields such as environmental and health monitoring, battle field surveillance, and industry process control. Sensor networks consist of sensor nodes, which are usually deployed in an ad-hoc manner and they self-organize and coordinate among themselves to perform a sensing task. The design of a WSN mainly focuses on extending the lifetime of the system since the sensor nodes work on battery. In contrast, energy constraints are secondary criteria to the traditional wireless networks like cellular networks. The architecture of WSN should be chosen in such a way that the network will be efficient in terms of energy consumption and should yield maximum lifetime for the network, while maintaining the required level of reliability for the data packets.

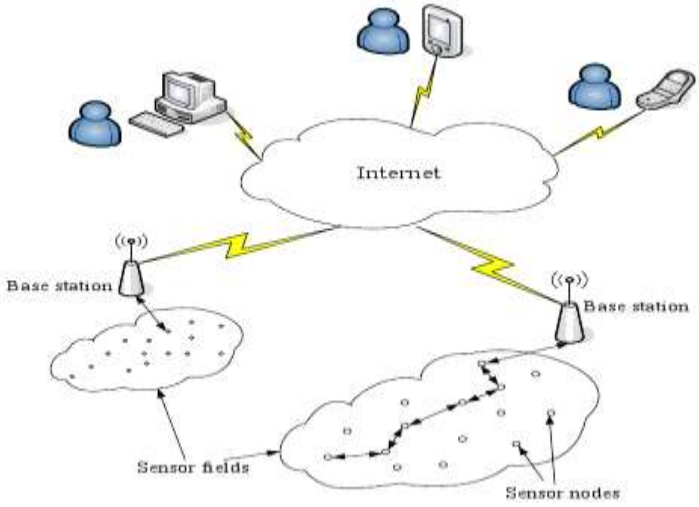

Figure 1: Accessing WSNs through Internet

Energy constraint is a prominent feature for WSNs, because sensor nodes consume available energy sources during sensing, processing and transmitting data in order to respond to the application requirements. These services are provided by the radio transceiver, which makes it the most energy consuming component of the node. In this context, defining new, innovative and up-to date solutions for energy consumption during data transmission is a necessity to increase the lifetime of the node and the network as well. Indeed, identifying energy dissipation sources during data transmission is important to develop suitable solutions for the energy consumption problem. Data are transmitted from one node to another through signal propagation, which is susceptible to different energy consuming problems, mainly packet collision, overhearing, interference and idle listening.

Sensor nodes are battery powered, which presents a limited resource. Based on the application requirements and the desired task, the lifetime of installed batteries varies from one node to another, depending on the computational effort. Once expired, batteries need to be replaced in time so the network does not break down. In some cases, node maintenance becomes complicated or even life threatening, like at military locations or where there is a danger of chemical explosion. This eventually results in permanent failure of the node, and that particular node is then discarded from the network operation.

Objective of this paper:

* To enhance network lifetime by implementing energy efficient path selection algorithm.
* To attain secure and reliable data transaction trust evaluation methodology has been deployed.
* Increasing network lifetime and achieving reliable data delivery with by pass approach.

II. LITERATURE SURVEY

Zhengwang Ye et.al (2017), presents Trust evaluation is an effective method to detect malicious nodes and ensure security in wireless sensor networks (WSNs). In this paper, an efficient dynamic trust evaluation model

(DTEM) for WSNs is proposed, which implements accurate, efficient, and dynamic trust evaluation by dynamically adjusting the weights of direct trust and indirect trust and the parameters of the update mechanism. To achieve accurate trust evaluation, the direct trust is calculated considering multi-trust including communication trust, data trust, and energy trust with the punishment factor and regulating function. The indirect trust is evaluated conditionally by the trusted recommendations from a third party. Moreover, the integrated trust is measured by assigning dynamic weights for direct trust and indirect trust and combining them.

Menaka A et.al (2020), proposed secure data transaction is focused through analyzing node trust. The challenge-response model promotes a focus on assessing trust for oneself; And linking it to its sub-center using the proposed self-survey and self-affirmation calculations, respectively. Hence node level trust is evaluated through self scrutiny and self attestation. Self scrutiny is analyzing every nodes self integrity level and self attestation evaluates the trust level of nodes that are included in transaction. In addition to this energy optimization has been implemented, to obtain this Energy Efficient Sensor Routing (EESR) protocol is implemented. This algorithm considers minimum path selection, energy utilization and node trust. To increase the performance based on energy factor, sleep and a wake approach has been used.

Farruh Ishmanov and Yousaf Bin Zikria (2017), presents routing is one of the most important operations in wireless sensor networks (WSNs) as it deals with data delivery to base stations. Routing attacks can cripple it easily and degrade the operation of WSNs significantly. Traditional security mechanisms such as cryptography and authentication alone cannot cope with some of the routing attacks as they come from compromised nodes mostly. Recently, trust mechanism is introduced to enhance security and improve cooperation among nodes. In routing, trust mechanism avoids/includes nodes in routing operation based on the estimated trust value. Many trust-based routing protocols are proposed to secure routing, in which they consider different routing attacks.

V.Bindu and Dr. Nithya.M (2019), describes the major issue in designing a network is to balance the energy consumption of nodes and to increase the lifetime of the network, by knowing that the nodes can be powered only by batteries in most of the conditions. Clustering is one of the most efficient methods to reduce energy consumption of nodes thereby to increase network lifetime. Here, Collision free secure clustering (CFSC) approach has been implemented. High connectivity cluster routing protocol has been implemented for data transaction where the cluster head is selected based on maximum remaining energy level of nodes. To overcome the traffic issues in delivering packets through CH, multi sink concept has been implemented. For secure data transaction in each cluster head IDS has been placed for trusted transaction of data and loss of data issues are also eradicated.

Ram Narayan Shukla, Rajesh Kumar Shukla (2013), To establish route between nodes, an efficient routing protocol is required to discover routes in a mobile adhoc network. Node energy is one of the important design criteria for adhoc networks due to dynamic topology of Ad Hoc Network. Mobile nodes have limited energy in their batteries. Power failure of a mobile node affects the node itself as well as decreases network performance also due to link failure. Much research efforts have been devoted to develop energy aware routing protocols. In this paper we propose an energy efficient routing algorithm that takes care about stability of network. A new route

discovery process proposed in this paper that takes into account the distance between nodes and node battery power to improve energy efficiency in AODV. This will maximize the network lifetime by minimizing the power consumption and decrease the routing overhead. We will implement our proposed algorithm in AODV and performance will evaluate against the original AODV.

Balakrishnan S et.al (2019), describes mobile Ad hoc Networks (MANET) is an autonomous collection of multi-hop wireless mobile nodes to establish communication without centralized infrastructure. Efficient routing protocol makes MANET reliable. Energy efficiency is a major problem of mobile Ad-hoc network as mobile nodes will be powered by batteries with limited capacity, insufficient source of energy and are difficult to replace or recharge. In MANET, Energy efficiency is an important challenge which leads to proposal of an Energy Efficient Enhanced AODV Routing Protocol that reduces delay, overhead, increases packet delivery ratio and consumes lesser energy compared to AODV.

III.PROPOSED WORK

In our proposed work, Energy efficient ad-hoc on demand distance vector (EEAODV) has been implemented where the path selection is done based on trust value of nodes included during path selection.

Route establishment:

In route establishment phase, the modifications has been done in processing and forwarding RREQ's which includes comparison of current threshold value of RSS with the received signal value. This comparison will decide whether this node will work as forwarding node or not.

Route handling:

In route handling phase, changes have been made in processing and forwarding route reply process. Here, the current RSS value of signal is compared with the threshold value. On the basis of it, transmission power of nearby node is reduced in the route reply phase.

Route Termination:

In the route termination phase, modifications have been made in route expiry process which in turn resets the transmission power of node.

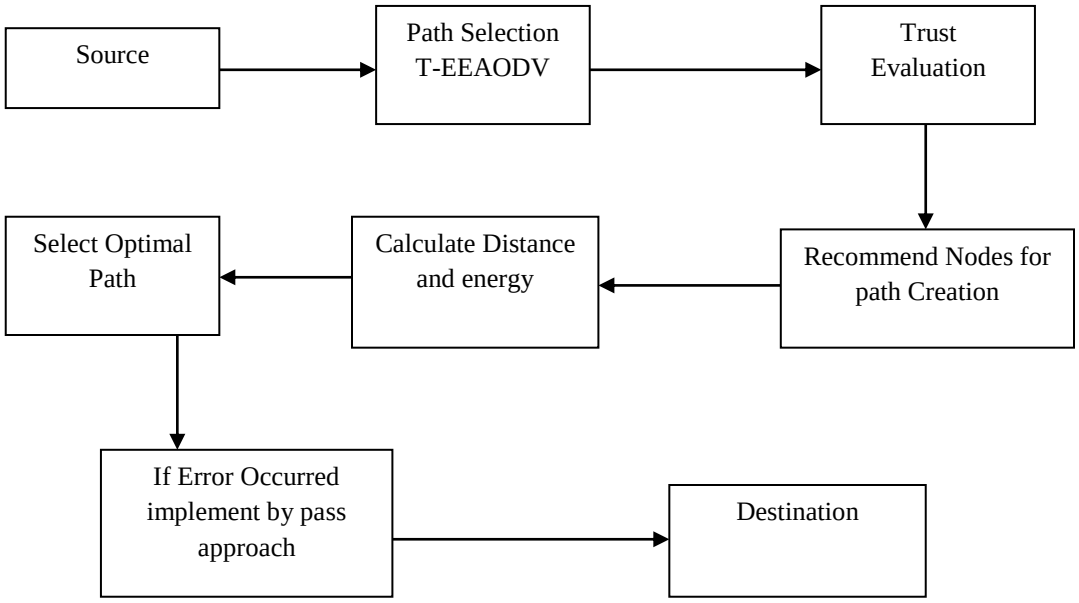

Figure 2: System architecture

The algorithm for EE-AODV is as follows:-

1. The process of path discovery gets initiated whenever a node needs to communicate with another node for which no routing information is present in its routing table.

2. Every node maintains two information in its routing table: route availability to another node and the energy consumption for that route.

3. Whenever a source node(S) sends RREQ to its neighbours for route discovery of the destination node (D), the neighbour node should send its energy level REPEL(Reply Energy Level) in response to that RREQ, if path to destination node (D) is available. If the path to destination node (D) is not available the neighbour node should send RERR.

4. If the source node gets REPEL from its neighbour which contains the threshold energy value or less than that, then discard that node from packet delivery till the time you have another option to send data.

5. After discovering the route from source to destination node, source node (S) should consider the neighbour which is having a path to destination node (D) as well as the maximum energy level as its next hop.

Energy Calculation:

Nodes involved in the delivery process of packets losses some energy after each transmit and receive. Let TP be the transmit Power for one packet, TT be the transmit Time of one packet, so, the amount of energy ET consumed during transmission of one packet will be:-

ET=TP x TT - (1)

Hence, Remaining Energy E_{new} of node will be,

$E_{new} = E_{curr}$ - ET -(2)

Similarly, let RP be the receiving Power for one packet, RT be the receiving Time of one packet,

so, the amount of energy ER consumed during receiving of one packet will be:- ER=RP x RT - (3)

Hence, Remaining Energy Enew of node will be,

$E_{new} = E_{curr}$ - ER -(4) With these calculations energy of the node at any interval of time can be calculated.

Trust Management:

Recently, trust management is used in several applications including routing, data aggregation, access control, and intrusion detection. The term trust management (TM) is used jointly with the terms trust establishment and reputation system. Trust establishment and reputation system are in fact parts of a TM system, and TM has a wider meaning. TM is defined as an entity, which addresses managing trust relationships, such as information collection, to make decisions related to trust, assessment of the criteria related to the trust relationship, and observation and reassessment of existing relationships. In the context of routing, TM deals with monitoring neighboring nodes during the transmissions, detecting misbehavior, estimating trust values based on detection results/recommendations, and propagation of trust value/recommendation.

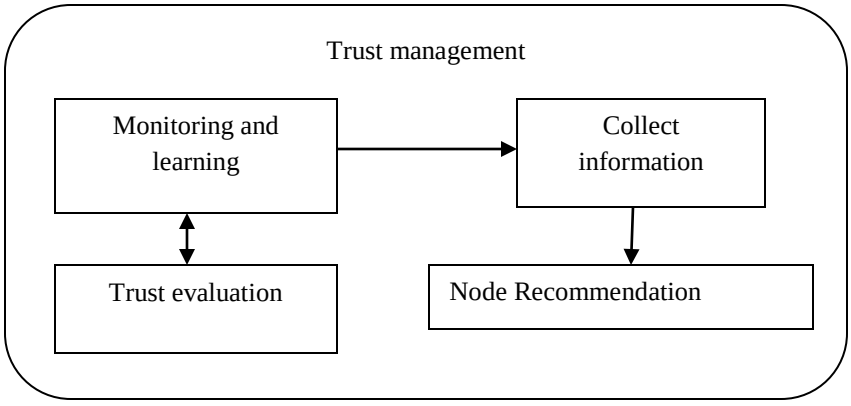

Figure 3: Trust management

Trust Evaluation: This is a central unit of the TM system, which performs estimation and integration of trust and reputation values, trust update, and so on. It provides output to the recommendation management unit.

Monitoring and Learning: Monitor and learn node behavior/performance and provide input to the trust evaluation unit. This is connected to a network interface to collect information about nodes.

Recommendation Management: This deals with the distribution and reception of recommendations (trust values). In addition, it provides trust values of nodes for various applications.

Trust Threshold: It is important factor in the attack detection and performance of trust establishment mechanism. Trust threshold is used to differentiate between malicious and benevolent node. Trust threshold is selected as about half of the maximum trust value, trust threshold is 0.5 when the maximum trust value is 1. Optimal threshold can be estimated by maximizing the false positive alarm rate while keeping false negative alarm rate to minimum.

Trust in Routing: Trust value plays direct role in route selection process. Each node maintains neighbor list along with corresponding trust value. Depending on the routing protocol trust is incorporated in a routing process in different ways to find a trustworthy routing path and avoid a malicious node. Route selection is performed either by source node or by nodes in the routing path.

According to bypass approach if any occurred during transaction of data in selected path then based on demand new path will be created with respect to condition verification. Therefore previous node will be considered as source node and data transmitted to destination. Hence our system ensures reliable data delivery between sources to destination.

IV.RESULT AND DISCUSSION

This section describes that our result attains maximum system performance compared to other existing approaches. Hence it was clearly described here; initially trust evaluation compared to other methods is shown below,

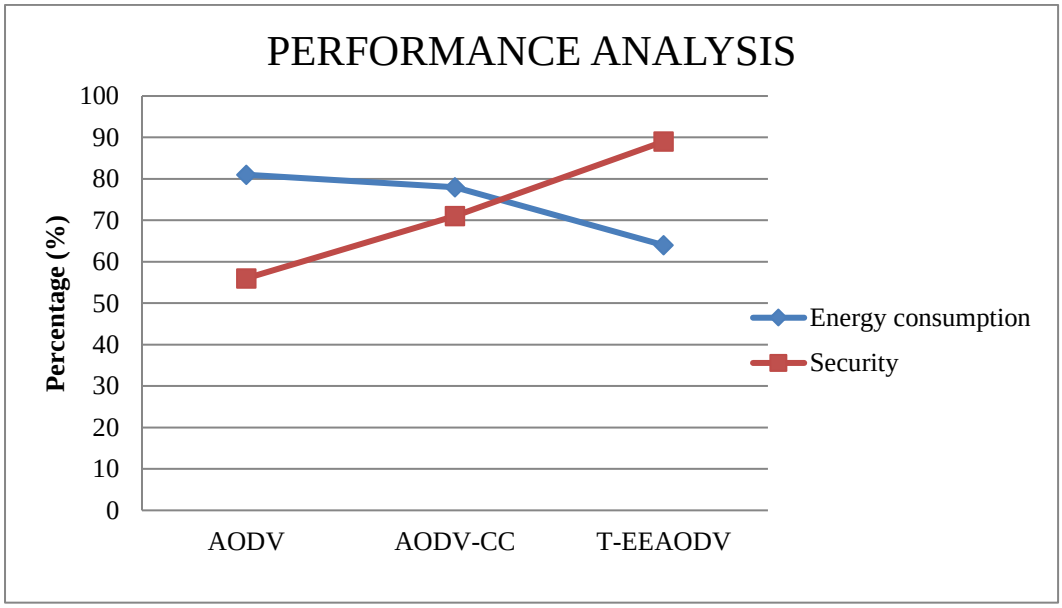

Figure 4: Performance analysis

The above graph clearly shows that our system achieves better result compared to other existing methods such as AODV and AODV-CC. energy consumption and security are the two major parameters compared and its outcome shows that our proposed achieves better result.

V.CONCLUSION

In WSNs, major issue focused is enhancing network lifetime and transmitting data from source to destination without any data loss. Hence trust based data transaction was implemented which reduces attackers node by evaluating node trust value and if its value is not up to threshold value it will not be included for recommendation. During path creation in our proposed work recommended node will be taken and its energy level and distance between source to destination was evaluated and optimal path will be selected through this data was transmitted. hence it shows that our proposed method achieves better result compared to existing approaches and it was clearly shown in result and discussion section.

REFERENCES:

[1] S. Prasanna and Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2 Issue-2, May 2012.

[2] Zhengwang Ye, Tao Wen, Zhenyu Liu, Xiaoying Song, and Chongguo Fu, "An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks" Hindawi Journal of Sensors Volume 2017, Article ID 7864671.

[3] Sabrine Khriji, Dhouha El Houssaini, Ines Kammoun and Olfa Kanoun, "Energy-efficient techniques in wireless sensor networks" Research gate November 2018.

[4] Menaka A, Jagadish R, Murali M, Bharathwaj R, Abinesh G, "Energy Optimized Node Level Trust Based Data Transaction in Wireless Sensor Network" international conference on advanced computing and communication systems (ICACCS).

[5] Farruh Ishmanov and Yousaf Bin Zikria, "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues" Hindawi Journal of Sensors Volume 2017, Article ID 4724852.

[6] V.Bindu and Dr. Nithya.M, "Enhancing Network Lifetime in WSN Using Collision Free Secure Clustering" International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454-9150 Vol-04, Issue-12, Mar 2019.

[7] Ram Narayan Shukla, Rajesh Kumar Shukla, "Improve Energy Efficiency in AODV" International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013.

[8] Ashwini H and Rajashri Y M, "Implementation of Energy Efficient AODV Protocol for Manet" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS051348 Vol. 4 Issue 05, May-2015.

[9] Jinghua Zhu, "Wireless Sensor Network Technology Based on Security Trust Evaluation Model" iJOE – Vol. 14, No. 4, 2018.