ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

A security Trust Mechanism for Transferring Packets to Sink Node in Wireless Sensor Networks

J.Joselin[1], V.S.Anita Sofia[2]

Research Scholar, Assistant Professor, Department of Computer Application,

Sri Krishna Arts and Science College[1]

Associate Professor, Department of Networking and Mobile applications,

PSGCollege of Arts & Science [2]

Abstract:

Routing concepts for wireless sensor networks (WSN) focuses ondistribution of packets from starting node to destination node . But security is an important drawbacks in the routing mechanism. Route of the network might be spoiled by intruder attack and suspension the activity of throughout of network. Cryptography and authorization being the solution for attack in WSN but these mechanisms are easily inactive by compromised nodes. So trust-based mechanisms are best solution to the sufficient security of routing. Trust is playing a important role in WSN to enhance the security. Trust management (TM) will ensure that all nodes are trustworthy during the routing. It finds the reliable and trustable node based trust value of each node and its neighbouring nodes. This paper introduced a new routing mechanism-based trust value of each node and it also evaluate the total path trust value..

Keywords: Cryptography, throughput ratio, end to end delay,packet delivery ratio, wireless sensor networks(WSN)

1. INTRODUCTION

The wireless sensor networks (WSNs) are developed with the overview of sensor nodes which are tiny, minimumof cost and accomplished of sensing, collaborating, and computing. The tracked results are aggregated to base station. Then the entire data are collected from base station and directed to user via Internet. A large number of nodes are set up in open and rigid locations to obtain data from sensor field. To supervise the area send the observed result to base station by enormousnumber of nodes collaborates with one. The capability of the node is limited by sensing area and message range, there is no choice but to cooperate with other nodes in the network. So the cooperation of the nodes is playing a vital role to evaluate the performance of WSNs. The factors that make WSNs susceptible to different attacks are their features such as open and harsh environment, open medium and several real time applications. Even though straight security mechanism such as cryptography and authentication can protect at some level, they alone cannot manage with negotiated node attacks.

2. ROUTES CHALLENGES IN WSN

Infrastructure-less networks that is why should give importance for routes.Large quantity of sensor nodes is needed to complete transformation.Data traffic has significant redundancy is occurred while transferring information. Generate same data from different sensors.Redundancy by the routing protocolsand Lot of new routing protocols have been expected

.3. DESIGN CHALLENGES IN WSNS

Due to insufficient availability of resources such as storage , bandwidth and energy there are some major design challenges in wireless sensor networks. The following requisites should be satisfied by a network engineer while designing new routing protocols[10].

Energy Efficient

Wireless sensor networks are mostly battery powered. Energy shortage is a core issue in this type of sensor networks especially in aggressive circumstances such as battlefield etc. When battery is droppedunder a pre-defined battery threshold level, the performance of sensor nodes is adversely affected [13]. While designing sensor networks, energy grants a main encounter for designers.

Complexity

The difficulty of a routing protocol may have an impact on the act of the whole wireless network[12]. The rationale overduethis is that we have inadequate hardware competences besides facing extreme energy limitations in wireless sensor networks.

Scalability

More number of sensors can be connected in wireless sensor network effortlessly since sensors are fetchinglow-costin everyday. Hence, the protocol of routing should sustenancethe miserable of network.

Delay

Some applications such asalarm checking orheat sensor needimmediateresponse or response lacking any considerable delay. Hence, the routing protocol must offer minimal delay.

In the quoted WSN applications the time required to transmit the sensed data need to remain as lesser as conceivable.

4. EXISITING METHOD

Fang et al(2021)[2]introduced single planar routing method. It has slow conjunction ratio for large scale WSN. Security and load balancing is very big challenges. This research proposed trust centered and little energy based hierarchical protocol (LEACH-TM). It used dynamic cluster head selection with lasting energy, number of nodes and energy consumption. It also focus the interioroutbreaks. The simulation result compared with LEACH-SWDN and LEACH. LEACH-TM perfectly secure the overall network.

Kalidoss et al(2020)[1] proposed new routing method. It is called as Secured Quality of Service (QoS) aware Energy Efficient Routing. In WSN energy consumption and security are the most important factor and it will give issues in multi-hop routing. Hence this research work focused designing of a protocol based on its trust and energy. Trust modelling of proposed work based on the authentication technique with key-based trust value. Cluster based secure routing is proposed. Final path routing is selected based on path trust,count of hop and energy. The simulation result evaluated by packet delivery ratio, and life time. Moreover this method produced better result than other security methods

Jedidi, A. (2020)[5] Developed trust history based protocol. nowadays quality of service is important with low cost, low - power consumption and high security is important inWireless sensor network (WSN). These three factors are important for QoS. But security is the very big challenge and issues in WSN designing. So this paper introduced a new security based method specially based on trust history of routing and routing path. So this algorithm ensure the high level security of routing path.

Keum, D., Lim, J., &Ko, Y. B. (2020) [3] proposed trust based multipath routing method. The tactical sensors and mission critical data are important things to confirm the consistency of soldiers. The mission critical facts should focus the prediction of exact situation for making decision. But malicious nodes may present in trust worthiness environment. Prediction of malicious node is the great challenges in mission critical data. the proposed method solve these issues and simulated in OPNET simulator. Simulation result produced better result than existing.

Saini, K., & Ahlawat, P. (2019) [4]designed a security and energy based routing algorithm. because low throughput, high path break ratio, low energy consumption are very big issues in WSN. This research work enhance security and efficiency of energy by fusion framework. It designed trust-based secure hybrid framework (TSER). It will produce a route with following factor secure,trustful and energy efficient. This method form the route based on lowest number of hop count, low energy consumption, authendication of each and every node. In the data transmission it will authendicate each node by replacing key messages. Then these are verified by base station. This method also focus the end to end delay while transferring data

5. PROPOSED METHOD

Total Path Trust Assessment Routing Method (TPTAR)

Step 1:Trust Value Evaluation:

Trust is have a confidence or relationship between two adjacent node. That is trustor believing trustee. There are two types of trust value prediction. (i) direct trust value ii) Indirect trust value.

This research work using both type of trust prediction.

(i) Direct Trust value(DTV_{xy})
Direct Observation obtained by the trustor about trustee
(ii) Indirect Trust value(RTV_{xy})
Indirect Observation or opinion gained from further nodes trust worthy third party

The Direct Trust Value (DTV) is calculated for each node in the network based on the following two sets. Once a node directs their acknowledgement to neighbors after receiving the packets it is measured as SET-1 node. When a node droplets more packets, it is measured as SET-2 node.

The trust Value (TV) for SET-1 is calculated using Equation (1)

$$TV_{S1y} = (ACKP/RP) \rightarrow (1)$$

where*TSS1y* - Trust value of node*j* when that one is SET-1,

ACKP is the number of acknowledgement packets conducted to the neighbors

RP is the quantity of packets expected from the neighbors group

The trust value for SET-2 is calculated using Equation (2).

$TV_{S2y} = 100-(NDP/TDP)*100 \rightarrow (2)$

where*TSS2y* is the Trust value of node *y* when this one is SET-2,

NDP is the number of packets plummeted

TDP is the total number of packets dropped in the network

The Trust value of node j is intended using Equation (3).

$TV_y = (TV_{S1y}+TV_{S2y})/2 \rightarrow (3)$

The Direct trust value of a node *x* in node *y* is denoted as

$DTV_{xy} = TV_y$WhereDTV_{xy}- direct trust value of node *x* trendy node *y*.

Step 2: Reference Trust Value(RTV)

The evaluating node may get other types of trust experience provided by some other node. It gets reference trust values about a knob from unalike adjacent nodes. A node assigns trust value depends on their individual experience with their adjacent nodes. The trustor gets the reference trust score from its neighbours. (TH) is the threshold value set by trustor by mean of the trust value of all nodes in the whole network.

Trustor consider the reference trust value of a node from their adjacent node greater than the threshold value(TH)

$$TH=\sum_{y=1}^{n} TVy/N \rightarrow (4)$$

After removing the reference standards, if more than one reference values are nominated then trustor takes the highest reference trust charge using Equation(5)

$$RTV_{xy=max}\{RTV_{ay}\} \rightarrow (5)$$

Where a is the adjacent node of y

Step 3:Total trust Rate(TTR)

The total trust rate is premeditated by summation of direct trust value and reference trust value as shown in equation 6

$$TTR_{xy=} DTV_{xy} + RTV_{xy} \rightarrow (6)$$

Step 4:Path Trust Value(PTV)

The route has been nominateddepends on the total trust value of the nodes from source (s) to destination (d) for transmitting the packets. The totality of the complete trust standards (TTR_{xy}) of the path is the path trust value (PTVsd) as given in Equation (14).

$$PTVsd=\sum_{s}^{d}(TTRxy) \rightarrow (7)$$

If variousroutes are obtainable between the starting and the terminus, then those routes path trust value are greater than the threshold value (*Th*) is selected. The *Th* is the mean value of the overall trust value entire nodes in the net.

$$Th=\sum_{\substack{x=1 \\ y=x+1}}^{n}(TTRxy) \rightarrow (8).$$

Conclusion:

All routing process are based on genuiness of the node and it should have energy effectual and nearby to sink node. But security of the routing is an added feature of the routing. Trust value evaluation techniques is used to predict the trust values. This research work introduced new technique to calculate the trust value.. From the result of experiment proposed method provides better performance than existing.

Reference:

[1]Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, *110*(4), 1637-1658.

[2]Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W., & Yang, Y. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digital Communications and Networks*.

[3]Keum, D., Lim, J., &Ko, Y. B. (2020). Trust based multipath qos routing protocol for mission-critical data transmission in tactical ad-hoc networks. *Sensors*, *20*(11), 3330.

[4]Saini, K., &Ahlawat, P. (2019). A trust-based secure hybrid framework for routing in WSN. In *Recent Findings in Intelligent Computing Techniques* (pp. 585-591). Springer, Singapore.

[5]Jedidi, A. (2020). Trust History-based Routing Algorithm to Improve the Quality of Service in Wireless Sensor Network. In *Communication, Signal Processing & Information Technology* (pp. 47-56). De Gruyter.

[6]Thippeswamya, BM, Reshma, S, Tejaswi, V, Shaila, K, Venugopal, K R &Patnaikd, LM 2015, 'STEAR: Secure Trust-aware Energyefficient Adaptive Routing in Wireless Sensor Networks', Journal of Advances in Computer Networks, vol.3, no.2, pp. 146-149.

[7] Tang, D, Li, T, Ren, J & Wu, J 2015, 'Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks', IEEE Transactions on Parallel and Distributed Systems, vol. 26, no.4, pp. 960-973.

[8]. Mahmoud, MM, Lin, X & Shen, X 2015, 'Secure and reliable routing protocols for heterogeneous multihop wireless networks', IEEE Transactions on Parallel and Distributed Systems, vol. 26, no.4, pp.1140-1153.

[9] Fang, W, Zhang, C, Shi, Z, Zhao, Q & Shan, L 2016, 'BTRES: Betabased Trust and Reputation Evaluation System for wireless sensor networks', Journal of Network and Computer Applications, vol. 59, pp.88-94

[10] Jadidoleslamy, H, Aref, MR &Bahramgiri, H 2016, 'A fuzzy fully distributed trust management system in wireless sensor networks', AEU-International Journal of Electronics and Communications, vol.70, no.1, pp. 40-49.

[11] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.

[12]J. Kaur, S. S. Gill, and B. S. Dhaliwal, "Secure trust based key management routing framework for wireless sensor networks," *Journal of Engineering*, vol. 2016, Article ID 2089714, 9 pages, 2016.

[13]P. Gong, T. M. Chen, and Q. Xu, "ETARP: an energy efficient trust-aware routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 469793, 10 pages, 2015.

[14]R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Enhanced trust aware routing against wormhole attacks in wireless sensor networks," in *Proceedings of the International Conference on Smart Sensors and Application (ICSSA '15)*, pp. 56–59, Kuala Lumpur, Malaysia, May 2015.

[15] A. Atayero and S. A. Ilori, "Development of FIGA: a novel trust-based algorithm for securing autonomous interactions in WSN," in *Proceedings of the International Conference on Computer Science Applications (ICCSA '15)*, IAENG WCECS 2015, pp. 174–180, San Francisco, Calif, USA, October 2015.