International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Trust Based Routing in Wireless Sensor Network

Madhu Patil, Goutham M.A

Abstract: ***The nodes are often placed in a hostile or dangerous environment so WSN will be vulnerable to security attacks. Attacks can be active or passive. Passive attack involves unauthorized attackers who listen to the communication channel and monitor its activities. In active attack, the unauthorized attacker's listens, monitors and alters the data passing through the communication channel. To address security concerns, cryptography approach has been adopted but this alone cannot cope with some of the routing attacks.***
As sensor devices are resource constrained, existing cryptography approach may not be applicable, due to the computational complexities that it involves [1] [3]. Hence, author present energy efficient trust based routing strategy, which is a viable alternative for WSN.

Index Terms: ***Direct trust, indirect trust, malicious node***

I. INTRODUCTION

In the context of WSN communication, node A will send message to node B for further transmission to the destination only if it has sufficient "trust" that node B will correctly forward the message. In this context, trust is a confidence level that ranges from 0 to 1, where 0 indicates absolute unreliability while 1 indicates absolute reliability. In a trust-based routing scheme, if node A wishes for forwarding to node B, will be done only if the trust that it currently assigned to node B is equal to or larger than a pre-specified threshold; otherwise, it would then consider some other node as a potential next node to which it would send the message for onward transmission to the destination node.

Clearly, node A must have some means of computing trust with respect to each of its neighbors. Such computation of trust involves two components, namely direct trust and indirect trust [4]. In the current context node A computes direct trust with respect to node B on the basis of its own observation of the correct transmission or otherwise of the messages that are received by node B for onward transmission. Each time node B receives a fresh message and either retransmits or else fails to retransmit the message, Node A updates its current direct trust value of Node B. Hence, this quantity is time-varying.

Indirect trust of node A with respect to node B involves the nodes that are in the vicinity of both .

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Dr. Madhu Patil*, Associate Professor, Department ECE, NMIT Blore. E-mail: madhu.patil@nmit.ac.in
Dr. goutham M.A, Professor and Head of Department, Department of ECE, AIT, Chickmagalur. E-mail: magoutham@gmail.com

Each such node C will have its own direct trust value with respect to node B and in turn node A will have a direct trust value with respect to node C. Both these quantities will be used by node A to compute its indirect trust value of node B with reference to node C [5]. The indirect trust values of node A with reference to all such intermediate nodes C are used to find a composite value of the indirect trust of node A with reference to node B. Direct trust and indirect trust is used for computing the overall trust of node A with respect to node B. The nodes have to forward the packet it receives. If it does not forward the packet to the destination it will be considered as not a well behaved node. The nodes spend energy while forwarding the packet. A behavior is treated as elfish if it does not forward the packet. These attacks are noted such as grey hole attack and black hole attack.

The proposed Security model considers the following setup, here homogenous wireless sensor network is considered. Each sensor devices monitor its adjacent devices and its packet transmission characteristic nature through mutual learning. The packet drop nature of defective and congested sensor device y follows Bernoulli distribution $B(y)$is expressed as follows,

$$B(y) = \begin{cases} 0 & y\ drops\ the\ data \\ 1 & y\ transmit\ \ the\ data \end{cases} \quad (1)$$

The faulty sensor devices may broadcast some faulty packets to determine as hop candidate for transmitting data packets but these faulty nodes drops the packet. The source and destination devices are not considered to be malicious and lastly once the network is deployed neither the sensor is added or removed from the network. The total trust degree is calculated both by direct and indirect trust computation [1-4]. Direct trust involves determining the packet forwarding behavior of node. Indirect trust uses recommendations from neighboring nodes. The packets are transmitted only through the trusted nodes.

II. RELATED WORK

As nodes are deployed in unattended environment, Wireless sensor networks are vulnerable to security attacks .Active and Passive attacks are the types of attacks.
Passive type of attack is listening and monitoring of communication channel by unauthorized attackers. In active attack the unauthorized attackers listens, monitors and alters the data in communication channel. This section provides survey of defending against some of the attacks such as Greyhole / selective forwarding, Sinkhole attacks, Sybil attacks and worm hole attacks.

TRUST MECHANISMS TO SECURE ROUTING AGAINST GREYHOLE/SELECTIVE FORWARDING ATTACK

In Selective forwarding attack some packets are dropped by the malicious node at arbitrary time.

The network performance gets degraded due to packet loss. A trust value for each node defines its trustworthiness with the neighbor nodes. It involves the following stages. First stage is monitoring of neighbor behavior. This involves monitoring and recording its neighbor's behavior such as forwarding of packet [5-9]. A popular monitoring mechanism is Watchdog [2] used in this stage.

TRUST MECHANISMS TO SECURE ROUTING AGAINST WORMHOLE ATTACK

The author in [5] proposed detection of worm hole attack in which if maximum range of transmission of the neighborhood node is greater than maximum range of transmission in the network than node is suspected as malicious node. *HELLO* Message is sent by source node thenode responds with appending HELLO message with presented received time and reply. The source node calculates distance between itself and destination. Worm hole is suspected if this distance is greater than the sender node maximum transmission capacity. Suspicious neighbor is ignored and alternate route is discovered. Distance is calculated by received time of HELLO message from neighbor. This mechanism requires tight clock synchronization.

TRUST MECHANISMS TO SECURE ROUTING AGAINST SINKHOLE ATTACK

Sink hole is an attack in which first malicious node attracts traffic by altered or replayed routing information. Then packets are selectively forwarded or tampered. Query Based routing protocol is proposed in [63]. In this sink node queries the network about the data that has to be broadcasted. The sensor node broadcasts the data after receiving the query. The nodes will forward the packets till it reaches the sink. Every intermediate node that receives the packets keeps record of trust value of the path, source node ID, sender node ID and number of hops covered. In this routing table all the possible routes are determined by considering the trust values of the paths between the sink and the source node.

TRUST MECHANISMS TO SECURE ROUTING AGAINST SYBIL ATTACK

Route selection process is performed in a distributive manner proposed in [10]. The trust value is used to select the neighbor node and energy,and cost of delivery of packet to send a packet to base station. Messages about lost packets are broad casted by base station. The node knows that the most recent period has ended and a new period has just started when a base station send broadcast message to the node. Due to energy consideration it is energy efficient. But, energy cost of packet delivery is reported by each node. Malicious nodes might exploit this to attract more traffic. Although such attack can be detected finally, it takes a long time to detect such exploit.

III. PROPOSED TRUST BASED ROUTING MODEL

The author presents trust based routing for wireless sensor network. Trust estimation is a key factor for trust based routing technique. Let us consider that every sensor devices has information of hop device ID, sender ID and receiver ID which are stored in buffer storage. Let us consider that sensor device x, y and z take part in transmission among source and end devices. Every sensor devices computes the degree of trustiness of its adjacent devices within its range of transmission.

The neighborhood trust parameter is computed using information experienced of adjacent devices. Let $T_{x,y}(t)$denote the overall degree of trust of the node x for node y at time instant t. The trustable parameter is in range of continuous fractional param [0,1], if trust param is closer to zero or zero the node is not trustable, similarly if the trust param is closer to one or one the node is considered to be safe/trustable.The overall trust $T_{x,y}(t)$ is weighted aggregated sum of direct and indirect trust which is depicted as follows

$$T_{x,y}(t) = m_{,}D_{x,y}(t) + m_{,,}\frac{ID^{z}_{x,y}(t)}{\mathbb{G}_{y}} \quad (2)$$

Where $ID^{z}_{x,y}(t)$depicts the mean trustable param indirectly gained by sensor device x using information from adjacent device z for sensor device y at instance t, $D_{x,y}(t)$represent direct trustable param by device x on y at instance t, and is calculated by using sensor device x, packet forwarding characteristic information of sensor device y. $\mathbb{G}_{y}$Depicts set of adjacent devices of sensor device y. Lastly $m_{,}$ and $m_{,,}$ are the weightage assigned to $D_{x,y}(t)$and$ID^{z}_{x,y}(t)$ respectively, such that $m_{,} + m_{,,} = 1$, where $0 \le m_{,} \le 1$and $0 \le m_{,,} \le 1$. The indirect trust is a parameter obtained from the adjacent devices who inform their direct trust param obtained from a specific device which is computed as follows

$$\sum_{z \in \mathbb{G}_{y,z \neq x}} ID^{z}_{x,y}(t) = \sum_{z \in \mathbb{G}_{y,z \neq x}} D_{x,z}(t) * D_{z,y}(t) \quad (3)$$

$D_{x,z}(t)$Represents the direct trust among sensor devices x and z and $D_{z,y}(t)$represent trustable parameter of direct trust computed by sensor devices z for sensor device y (which are the common neighbors of nodes x and y).

The indirect trust by the recommendation of other nodes will speed up the convergence rather than the direct trust method. However sharing the trust information will lead to security vulnerability. To address this the sensor device obtain information directly from adjacent devices whose trust param is greater than or equal to defined threshold (0.5). Trust degree for well behave nodes increase linearly with time. Similarly, trust degree values for misbehaving nodes decreases as the simulation proceeds. It is due to fact that trust rating for well behaving nodes incremented each time as it cooperates in packet forwarding.

COMPUTATION OF NODE TRUST

In this section the method of estimating the direct trust is discussed. The direct trust of node is calculated using packet forwarding behavior. This means all the packets received by node should be forward successfully. At time t the direct trust, $D_{x,y}(t)$ is computed by observing the characteristic of adjacent devices. To compute direct trust, packet forwarding ratio is considered which is as follows

$$D_{x,y}(t) = F_{x,y}(t) \,/\, R_{x,y}(t) \quad (4)$$

Where $F_{x,y}(t)$is the total packets forwarded at time $t$by node y. $R_{x,y}(t)$is the packets received successfully by node y at time t. Every time a node receives a packet from neighboring node $R_{x,y}(t)$ incremented by 1. Similarly, every time the node successfully forwards the received packets to intended destination, $F_{x,y}(t)$ is incremented by 1.

When trusted sensor device is selected for forwarding packet, high throughput is achieved.

The cost function (O) of proposed routing is defined as follows

$$O = w1 * T + w2 * E \quad (5)$$

The weightage $w1$, $w2$ depicts the impact of trust and remaining energy E respectively, where $w1 + w2 = 1$. The sensor device that satisfies this optimization will be chosen as a device for transmission. The incorporation of energy param in routing strategy aid in choosing the trusted node whose remaining energy is higher than predefined threshold thus improving the security and energy efficiency of proposed model. The node whose cost function O is greater than or equal to 0.5 is selected as a hop device for transmission

IV. SIMULATION RESULTS

Windows 10 enterprises 64-bit operating system with 12GB of RAM.is the system environment used. Author has used sensoria simulator which is a dot net based simulator that uses C# as a programming language. Simulation studies are conducted to obtain performance in terms of the following parameters routing length, processing delay and communication overhead. The proposed trust based routing protocol is compared with Low Energy Adaptive Clustering Hierarchy $(LEACH)$ for different node size.

Initially, all sensor device are considered to be trustable i.e., its threshold is assigned with 1.For every 0.1 seconds, randomly the sensor device sense for packet (temperature data is considered) and this information is sent to its cluster head device which in turn transmit it towards the sink. During transmission if any node fails to transmit the data the trust parameter is decreased by 0.1. The value of trust parameter is between 0 to 1).The value closer to 0 represent least trusted or faulty node and the value closer to 1 is considered to be trusted node).The threshold parameter is dynamic with respect to application security level requirement. The node that has threshold value lesser than 0.5 is considered to be faulty nodes and these nodes are eliminated from routing path.

Routing length is measured in terms of how may hop device it uses to transmit a packets form source (sensor device) to the sink. The time taken for message to be transmitted from source towards sink is measured by a processing delay in seconds. The model eliminates the scenario of message loss due to faulty nodes. The amount of energy incurred for communicating packet loss information to the base station through control channel is measured by communication overhead

In the secure routing approach of proposed model, the effect of routing length (number of hops) due to secure path is presented in Figure 1. The routing length for the $LEACH$ system is high for all network size such as 500, 1000 and 2000 nodes. While the proposed model without using security approach routing length is less than the proposed model with security. In security approach of the proposed model routing length is more due to finding a secure way but its routing length is less than that of $LEACH$. An average reduction of 37.86% and 41.12% of routing length is achieved for with and without security of proposed model respectively over exiting $LEACH$ protocols.

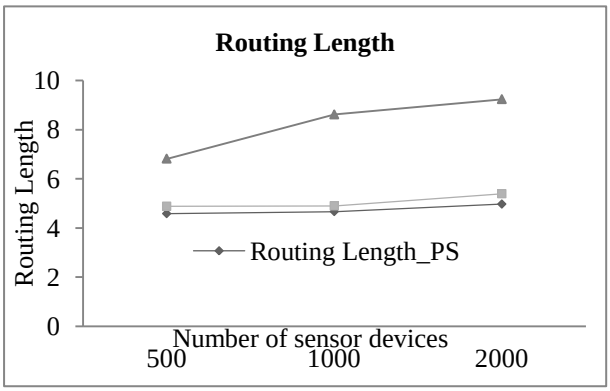

Figure 1-Network RoutingLength

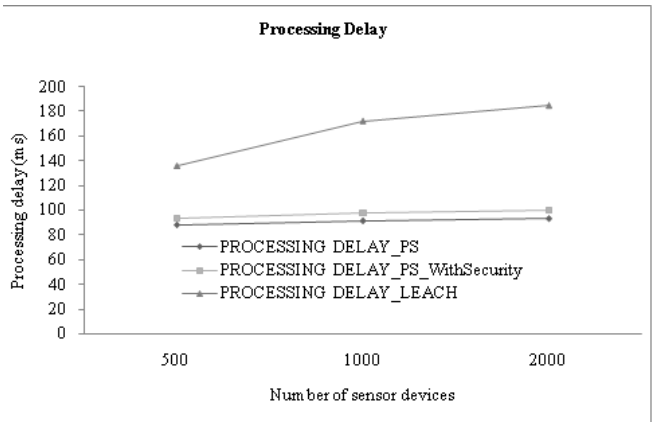

Figure 2-Processing delay

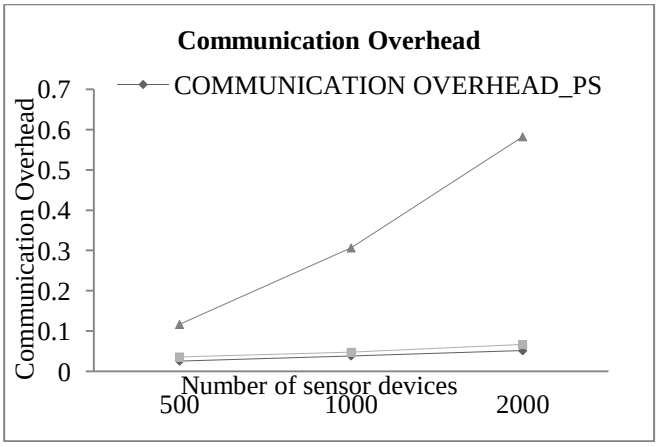

Figure 3-Communication overhead

Processing delay among source and destination due to secure path is presented in Figure 2. Here it is observed that the packet processing delay for the $LEACH$ protocol is high for all network size such as 500, 1000 and 2000 nodes. While the proposed model without using security approach packet processing delay is less than the proposed model with security.

In security approach of the proposed model packet processing delay is more due to finding a secure way but its packet processing delay is less than that of *LEACH*. An average reduction of 41.27% and 43.81% of processing delay is achieved for with and without security of proposed model respectively over existing *LEACH* protocols.

In the secure routing approach of proposed modeling, effect of communication overhead in network due to secure path is presented in Figure 3.

Here the communication overhead for the *LEACH* protocol is high for all network size such as 500, 1000 and 2000 nodes. While in proposed model without using security approach packet processing delay is less than proposed model with security. In security approach of proposed model communication overhead is more due to finding a secure way but its communication overhead is less than that of *LEACH*. An average reduction of 80.75%and 85.49% of communication overhead is achieved for with and without security of proposed model respectively over existing *LEACH* protocols.

V. CONCLUSION

The nodes are often placed in a hostile or dangerous environment so WSN are vulnerable to security attacks. Here energy efficient trust based routing is proposed. The direct trust of a node based on packet forwarding behavior is evaluated. A node with high trust value nearer to 1 is trusted node. Such a trusted node always forwards the packets it receives. This depletes the energy of the trusted node. So to select the node for routing trust values of node as well as remaining energy of node is considered.

Routing length, processing delay and communication overhead are the parameters analyzed for energy efficient trust based routing.

REFERENCES

1. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00), pp. 255–265, August 2000
2. Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 205920, 16 pages, 2013.
3. A. Josang and R. Ismail, "The beta reputation system," in Proceedings of the the 15th Bled Electronic Commerce Conference, June 2002 [53]Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 205920, 16 pages, 2013.
4. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2-3, pp. 293–315, 2003.
5. H.Deng, X. Sun, B.Wang, and C. Yuanfu, "Selective forwarding attack detection using watermark in WSNs," in Proceedings of the Second ISECS International Colloquium on Computing, Communication, Control, and Management (CCCM '09), pp.109–113, August 2009..
6. S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusion detection systemforWSN," in Proceedings of the 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN '15), pp. 183–188, Islamabad, Pakistan, September 2015.
7. 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.
8. J. Harbin, P. Mitchell, and D. Pearce, "Wireless sensor network wormhole avoidance using reputation-based routing," in Proceedings of the 7th International Symposium on Wireless Communication Systems (ISWCS '10), pp. 521–525, IEEE, York, UK, September 2010.
9. H. Liang, H. Fan, and F. Cai, "Defending against wormhole attack in OLSR," Geo-Spatial Information Science, vol. 9, no. 3, pp. 229–233, 2006.
10. X.-F. Qiu, J.-W. Liu, and A. R. Sangi, "MTSR: wormhole attack resistant secure routing for Ad hoc network," in Proceedings of the IEEE Youth Conference on Information, Computing and Telecommunications (YC-ICT '10), pp. 419–422, Beijing, China, November 2010.
11. A. Pirzada, A. Datta, and C. McDonald, "Propagating trust in ad-hoc networks for reliable routing," in Proceedings of the International Workshop on Wireless Ad-Hoc Networks, Oulu, Finland, June 2004.
12. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF. RFC 3561, July 2003.
13. O. Naderi, M. Shahedi, and S. M. Mazinani, "A trust based routing protocol for mitigation of sinkhole attacks in wireless sensor networks," International Journal of Information and Education Technology, vol. 5, no. 7, pp. 520–526, 2015.
14. S. D. Roy, S. A. Singh, S. Choudhury, and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," in Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC '08), pp. 537–542, IEEE, Marrakech, Morocco, July 2008.
15. P. Samundiswary and P. Dananjayan, "Secured dynamic source routing protocol for mobile sensor networks," in Proceedings of the 12th International Conference on Networking, VLSI and Signal Processing, pp. 19–23, Cambridge, UK, February 2010.

AUTHOR PROFILE

Dr.Madhu Patil currently working as Assoc Prof, in Dept ECE at NMIT Blore . Her areas of interest are communication and signal processing **madhu.patil@nmit.ac.in**

Dr. goutham M.A is currently working as prof and head of ECE Dept at AIT, Chickmagalur. His areas of interest are Signal Processing, Communication and MEMS. **magoutham@gmail.com**