Journal of Theoretical and Applied Information Technology
10th April 2015. Vol.74 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MALICIOUS NODE DETECTION THROUGH TRUST AWARE ROUTING IN WIRELESS SENSOR NETWORKS

[1]RAJA WASEEM ANWAR, [2] MAJID BAKHTIARI, [3]ANAZIDA ZAINAL and [4]KASHIF NASEER QURESHI

[1] Department of Communication, Faculty of Computing, University Teknologi Malaysia, Skudai, 81310, Johor Darul Takzim, Malaysia

E-mail: [1]rajawaseem@gmail.com , majid, anazida@utm.my, kashifnq@gmail.com

ABSTRACT

Wireless sensor network are constituted by a large number of tiny size sensors and distributed randomly for gathering information. These types of networks have remarkable applications and demand worldwide. The wireless sensor network has been suffered with variety of attacks because of its design and deployment nature. The previous traditional approaches including cryptography, authentication cannot work properly against node misbehavior attacks. To solve this problem, we propose a Trust Aware Wireless Routing Protocol (TAWRP) for detection and isolation of malicious nodes in network. The main aim of TAWRP is to establish an optimal route with trusted nodes and effectively forward the packets from source to destination with minimum packet loss. The performance of TAWRP is evaluated in terms of packet delivery ratio and routing overhead. The results clearly showed that TAWRP can achieve high delivery ratio and efficient in routing overhead in the presence of malicious nodes.

Keywords: *Sensor Nodes, Malicious, Trust, Overhead*

1. INTRODUCTION

A Wireless sensor network (WSN) is an emerging, self-organized, inexpensive network for sense gather and measure environment information and transmit to the user. This type of network gained worldwide attention because of smart functions with limited processing and computing resources. These small tiny size sensors provide unprecedented opportunities and communication capabilities through wireless links. These sensors are used in variety of applications such as defense areas, environmental monitoring, transportation, smart homes, and disaster management, etc [1, 2]. The sensor nodes equipped with low power battery, a processor, radio, memory, and an actuator and different types of mechanical, biological, magnetic sensors attached to monitor and measure different properties. These nodes are deployed unattended in hostile environment and this gives an ideal opportunity to an attacker to intrude the system. Various different security mechanisms, techniques and protocols have been proposed to avoid security threats such as malicious node detection, DoS attacks, and applied for routing data between source and destination in these networks but WSN still suffer from many security threats and vulnerabilities. Sometime selfish and malicious nodes disturb this process of routing and violate the protocols regulations. These different types of attacks in WSN are categorized into two main type's namely internal and external attacks. The attack on key information and authentication are belonging to external attacks. In order to encounter with these external attacks various approaches are used such as cryptography, authentication and encryption these approaches and methods resist against external attacks, but cannot solve internal attacks which occurs due to compromise node by an adversary results in node misbehaving which further lead to blackhole attack, sinkhole attack, etc. [3, 4]. The typical approaches cannot work to address these internal attacks in network.

The paper is organized as follow: the section two illustrates existing traditional security issues in the context of wireless sensor network and section three presents related work. In section four briefly describe the proposed routing protocol with analytical framework. The last section five present the numerical results in terms of packet delivery ratio and routing overhead.

Journal of Theoretical and Applied Information Technology
10th April 2015. Vol.74 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. ISSUES WITH TRADITIONAL SOLUTIONS

Many researchers proposed various secure solutions for enhance the performance of WSN and protest from malicious node and from different attacks. Most of existing solutions are based on cryptography and authentication techniques but these solutions need central administration for security. In WSN environment the central administration is not available [5]. In cryptography solutions an authorized compromised node can easily access to valid secret key and memory contents and need high energy, memory and computation. The previous security systems dealt with PKI X.509 [6], PGP [7], and designed for finding trustworthy copy of public key of someone.

3. RELATED WORK

To address these issues with traditional security solutions the concept of trust has been proposed. The concept of trust management in ad hoc sensor network is an efficient tool to handle node misbehavior attacks in network. Trust is integrated component in everyday life, in the context of computer science there are many defamations used and differ with application areas. In a broad manner trust is an essential component for semantic web. According to previous work the trust is the degree of belief about the future behavior of other entities [8, 9]. The first time Blaze, Feigenbaum and Lacy [10] used the term trust management and introduced as a separate security component. There are many trust aware routing approaches have been proposed to detect malicious nodes in network. In 2013 [11] author proposed a trust model and combine each node direct and indirect trust information to define the trustworthiness of all its one hop distance neighbors. The proposed ATSR protocol adopts location based approach to reduce processing, storage. Protocol performed on hop-by-hop basis and next hope selection based on balancing of routing and security criteria. Author claimed that his proposed model reveals malicious nodes even though with different attacks and defines alternative trust based route to the destination. However, in the case of high mobility of nodes this approach takes time for establishing trust between nodes.

In another [12] trust based approach author used repeated games for detection malicious nodes. The role of repeated game strategy in wireless sensor network calculated the average number of dropped packets verses discount payoff. The model is useful to transfer the packets with minimum overhead. Basically the game theory is a bi-directional and WSN is a one way transmission where sensor nodes send the data to base station. In this situation this approach is not helpful because of non-predictive nature of wireless network. Chakraborty, et al. [13] addressed the problem of malicious adversaries in WSN through three tiered trust based architecture. The proposed approach differentiates legal and illegal sensor nodes and filters out forged and deceitful data. However, this approach is without monitoring mechanism and for managing secret key it need some extra computation and storage.

Theodore, et al.[14] proposed a trust aware location based routing protocol named ATSR (A Trust Aware Routing Protocol). It protect network with malicious nodes and support large scale nodes deployment. In this approach the nodes monitor neighboring node behavior and evaluate trustworthiness before forwarding. This protocol also consider indirect or reputation trust information and direct and indirect information merged to calculate total trust and geographical information. The issue with this protocol is network overhead due to direct and indirect information and nodes compute extra processing.

4. PROPOSED APPROACH

In this section we described proposed protocol TAWRP which secures the multi-hop routing in wireless sensor network and work against node misbehaviors by evaluating the trustworthiness of neighbor nodes. The proposed approach is based on four steps: Information Gathering, Trust Analyzing and ranking, Route Discovery and Route Selection.

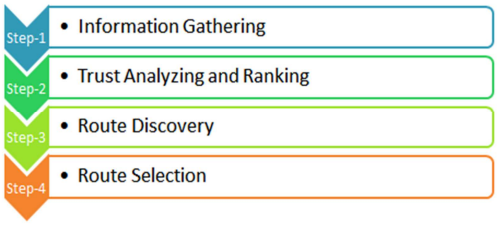

Figure 1: Steps For Proposed Approach

In the first step, behavioral information about the sensor network is collected based on the node interactions with its neighboring node. In the second step trust analyzer checks the trustworthiness of sensor nodes in network. The third step discovers the route based on trust information and finds a suitable route. In last the route selection is finalized and source node sends the packet to destination and established a trusted

Journal of Theoretical and Applied Information Technology
10th April 2015. Vol.74 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

route. The trust analyzer checks the trustworthiness of neighbor nodes and identifying nodes misbehavior in network. After monitoring phase the data will forward and store in trust database. The next step is route discovery to find shortest, trusted and reliable route. Each nod in network relies on neighbor node to select an ideal and reliable route based on trust level. If neighbor node is below a certain threshold then it will be excluded from forwarding candidate selection. Our proposed approach prefers the forwarding node with higher trust value, because of this value and trustworthiness efficiently protect the network from an adversary node in network. The last step of proposed approach is selection of route after discovery as shown in figure 2.

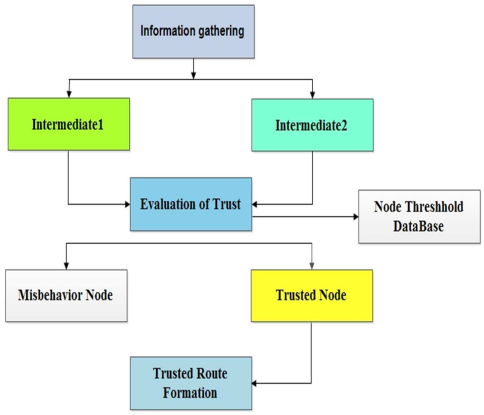

Figure 2: Proposed Approach Steps

In this procedure route will be established and packet forwarding process is carried out. In below section we discuss the all steps of proposed protocol in detail.

4.1 Analytical Framework

We model the sensor network as a graph G = (V, E, M), where V denote sensor nodes and E represent the nodes between source and destination and M denote metrics used in protocols. The trusted route R contain set of trusted sensor nodes denote with s, d, m,n, (s,d) ∈ V and n (s, d) ∈ E (s is sender node, d is destination node and m is misbehaving node). The m node is misbehaving node and cause of packet drop and congestion in network.

$$A(m) = \begin{cases} 1 & m\ Forwarded\ packets \\ 0 & m\ drop\ packets \end{cases} \quad (1)$$

The first step of proposed protocol is trust analyzer for trustworthiness of neighbor node and checks its transmission and dynamically identified misbehavior of nodes and stores the results in trust database. In the below equation the node s evaluate trust of node d as T_{sd} in Equation

$$T_{sd} = \alpha \times T_{sd}intermediate1 + \beta\ T_{sd}^{m}intermediate2 \quad (2)$$

$T_{sd}intermediate1$ represents the intermediate neighbor trust node, which is observed by s for node d. on the other hand $T_{sd}^{m}intermediate2$ denotes the average degree of intermediate trust node which is come from s neighbor m for node d. The α and β represents the weight factors, which are assigned to $T_{sd}intermediate1$, $T_{sd}^{m}intermediate2$ respectively. The weight factor shows the values such as $\alpha + \beta = 1$, and always set the value of α is higher than β.

In discovery step the proposed protocol calculate the packet forwarding ratio to discover the optimal route. The misbehaving node is cause of packet delay and through this step the route is selected on the basis of packet forwarding ratio.

$$T_{s,d}intermediate\ 1 = \sum_{p=0}^{N-1} Forward\ packts\ (p) \Big/ \sum_{p=0}^{N-1} Recieved\ packts\ (p) \quad (3)$$

The equation (3) shows the trust weight calculation for discovery step, where every time source node calculates received packets from intermediate node with increment 1 and every time node successfully forwards to destination with increment 1. From this packet forwarding ratio trust model at node s present the well or malicious behavior of node d. If the value is above specified threshold the node considered as trusted node, otherwise it will be malicious. If any misbehaving node disturb the data the packet forwarding value is decrease and source immediately stop and discard this route and again start the discovery step to find another trust worthy route for data forwarding.

The last step is route selection where source node select an optimal route after two steps and ready to send packets to destination without any delay.

5. NUMERICAL RESULTS

We use NS2 [15] simulator to analyze the performance of proposed TAWRP (trust aware wireless routing protocol). In simulation setup we

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

consider a misbehaving node in network to send fake or malicious route discovery packet to disturb the routing process. In the presence of malicious node the network is congested and the delivery of packets will disturb. We test our proposed approach with TARF (trust-aware routing framework) [16], which is latest trust aware routing protocol in WSNs. The Table 1 below shows the simulation parameters.

TABLE 1: SIMULATION PARAMETERS

S/ No	Parameters	Value
1	Simulation area	600m × 800m
2	Sensor nodes	35
3	Malicious nodes	0-3
4	Mac Layer	IEEE 802.15.4
5	Packet Size	1000 bytes
6	Simulation Time	1000 Sec
7	Packet forwarding threshold	0.4
8	Trust Threshold	0.8

In first experiment we analyze the average degree of trust estimation of normal and malicious nodes behavior. After this we test the proposed TAWRP protocol with TARF in terms of packet delivery ratio, end-to-end delay and routing overhead. The Figure 3 shows the trust estimation mechanism of proposed trust routing protocol. It is clearly shows that the trust oriented sensor nodes trust is increase with time and on the other hand with misbehaving nodes the value is dropping.

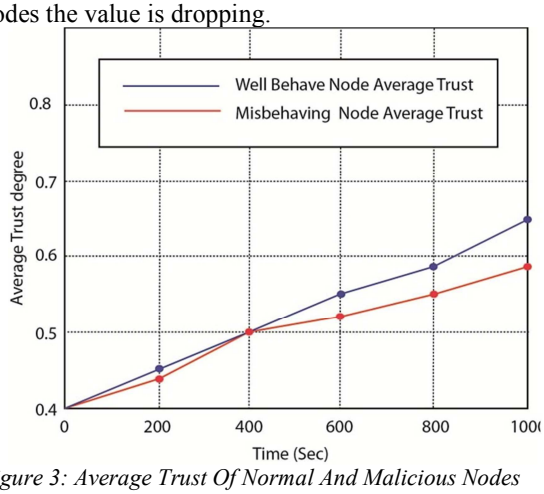

Figure 3: Average Trust Of Normal And Malicious Nodes

The Figure 4 shows the performance of proposed TAWRP and TARF in terms of packet delivery ratio against number of malicious nodes in network. The results clearly shows when the number of malicious nodes increase in network packet drop ratio of TARF is more compared with proposed TAWRP protocol. When we add 5 malicious nodes in network then the packet delivery ratio of TAWRP average is 60 and TARF ratio is 40.

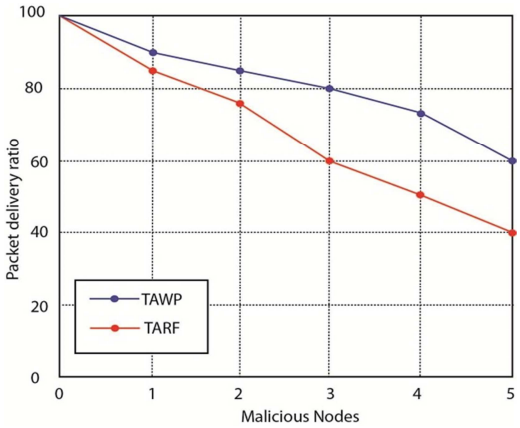

Figure 4: Packet Delivery Ratio With Malicious Nodes

The network routing overhead is also increase in the presence of malicious nodes in network. The Figure 5 clearly shows the better results of proposed TAWRP compared to TARF. The routing load is a significant factor during designing a wireless sensor network protocol.

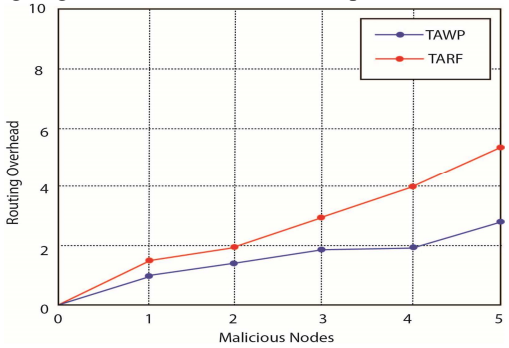

Figure 5: Routing Overhead With Malicious Nodes

6. CONCLUSION

Trust aware routing in wireless sensor network have been gain extensive attention of researchers and widely used to address the issues of node misbehavior in network. In order to isolate malicious node in a network a little contribution is done with proposed trust aware wireless routing protocol (TAWRP). The numerical results clearly showed the malicious nodes affect the overall performance of network in term of packet delivery ratio and routing overhead. TAWRP enhance the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

overall performance of network and isolate the malicious nodes. In future we plan on broadening our work with more complex network scenarios enhancement of the proposed protocol and to improve trust among sensor nodes by considering more trust metrics, such as node energy consumption, hop-count and path quality.

REFERENCES:

[[1] K. N. Qureshi and A. H. Abdullah, "Wireless Sensor Based Hybrid Architecture for Vehicular Ad hoc Networks," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 12, 2014.

[2] Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., & Qureshi, K. N. (2014). Security issues and attacks in wireless sensor network. World Applied Sciences Journal, 30(10), 1224-1227.

[3] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, pp. 867-880, 2012.

[4] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," 2006.

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 8, pp. 1086-1090, 2009.

[6] D. Cooper, "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile," 2008.

[7] P. R. Zimmermann, The official PGP user's guide: MIT press, 1995.

[8] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, 2000, p. 9 pp. vol. 1.

[9] D. Gambetta, "Trust: Making and breaking cooperative relations," 1988.

[10] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on, 1996, pp. 164-173.

[11] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," Wireless personal communications, vol. 69, pp. 805-826, 2013.

[12] Y. Reddy and R. Selmic, "A Trust-based Approach for Secure Packet Transfer in Wireless Sensor Networks," International Journal On Advances in Security, vol. 4, pp. 198-207, 2012.

[13] A. Chakraborty, V. Parekh, and A. Ruia, "A Trust Based Routing Scheme for Wireless Sensor Networks," in Advances in Computer Science and Information Technology. Networks and Communications, ed: Springer, 2012, pp. 159-169.

[14] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, et al., "Design and implementation of a trust-aware routing protocol for large wsns," International Journal of Network Security & Its Applications (IJNSA), vol. 2, pp. 52-68, 2010.

[15] J. Zheng and M. Lee, "NS2 Simulator for IEEE 802.15. 4," ed, 2004.

[16] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs," Dependable and Secure Computing, IEEE Transactions on, vol. 9, pp. 184-197, 2012.