International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

An Improved Combined Bandwidth-Trust Secure Routing Framework

Mir Aamir Rasool† and Birinderjit Singh‡

†Electronics and Communication, SVIET Banur affiliated to P.T.U Jalandar, Punjab India

Accepted 15 July 2015, Available online 17 July 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

In recent past, trust aware protocols play an important role in security of wireless sensor networks(WSN),which is one of the common network technologies for smart city. However along with trust only distance metric was considered but some important metrics such as bandwidth were not included in conventional trust aware routing protocols. These excluded metrics are important for higher throughput and efficiency. In our thesis we will use these metrics in addition to distance and trust for our route selection. Besides this some nodes are attacker nodes, while finding the route from source to destination we will bypass that node.

Keywords: *Wireless Sensor Networks, Trust, Bandwidth, Malicious Nodes.*

1. Introduction

Wireless sensor networks (WSN) provide solutions that accommodate broad range of applications arena , including homeland security and public healthcare, building and urban surveillance, industrial operations and environmental monitoring (Son, B., Her, Y., Kim, J., September 2006),(Mainwaring *et al*,Sep. 2002),(Chintalapudi, K.; Fu, T.; Paek, J,March-April 2006),(Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury,March 2007). Their increasing incursion mainly stems from three key advantages: wireless operation, low cost and easy installation/ self-organization. However security issues are introduced by these advantages (V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi,2008).

A number of security attacks are presented in the literature with a important subset disturbing the routing process (T.Kavitha, D.Sridharan,2010), (Jaydip Sen, August 2009). Once an antagonist node manages to take part in the network, the routing process can be damaged by simply dropping the packets that need to be forwarded , i.e. denial for sincere cooperation in the routing process. Packet modification is another type of attack. A classification of routing attacks can be found. An approach has been proposed to avoid such routing attacks. Each node evaluates the trustworthiness of its neighboring nodes by continuously keeping them on surveillance.

Due to limited range of radio communication, wireless sensor nodes usually communicate with each other through a multi-hop path. In this case the key process is to design a routing protocol that determines the data forwarding and transmission path because it will directly affect the performance of WSN's like network lifetime packet delivery rates and delay (B. C. Villaverde, S. Rea, and D. Pesch,2012),(D. A. Tran and H. Raghavendra,2006). In this paper, we concentrate on security and speed aspects of routing protocols in WSNs. Because of open, distributed, and dynamic nature of WSN's, the routing protocols are extremely insecure to various attacks. These attacks are of two types: internal and external. The internal attacks are caused by malicious nodes in the network. The external attacks are caused by malicious nodes that don't have access to the network .Different routing protocols have been developed over years to protect WSN's from malicious and selfish behavior . But these routing protocols depend on cryptographic or coded primitives and authentication mechanisms that are not suitable for WSNs (M. L. Das, 2009).

This security system may become ineffective if the keys are leaked. It means conventional secure routing protocols can protect few types of external attacks, but cannot protect against malicious behavior of internal nodes. The effective solution to the above issues is trust management and it could form an essential component for security architecture of WSN's. The results of trust evaluation will help the source node to find the next node in network that is trust worthy through which it can forward the packet to destination node. As a result, a number of trust-based routing protocols have been proposed (G. Zhan, W. Shi, and J. Deng, 2012). However, in the traditional trust-based routing protocols their still exist several key problems, which can be summarized as follows. Firstly, although the trust-based schemes can deal with the inherent attacks in wireless networks, they will also induce some new risks to which special consideration shall be given. Secondly,

*Corresponding author: **Mir Aamir Rasool; Birinderjit Singh** is working as Assistant Professor

trust metric is significantly different from normal routing metrics such as the number of hops, delay, or other QOS requirements, but most trust models do not consider the particularity of trust metrics when designing routing protocols (Marti, T. J. Giuli, K. Lai, and M. Baker, August 2000). Thirdly, the existing trust-based routing protocols have some limitations such as dependence on specific routing scheme or platform.

1.1Trust Computation of Nodes

In terms of computational power, energy, memory, and bandwidth, the sensor nodes are highly constrained hence, the design of security mechanisms used for WSNs is significantly challenging. To evaluate the trust value of sensor nodes in WSNs we first propose a light weight computation method. Trust can be calculated using the formula

$$t(i,j)^l = \alpha \times dt(i,j)^l + \beta \times \frac{\sum_{(K\in C_j, K\neq i)}^{n} it(k,j)^l}{n-1} \quad (1)$$

Including α+β=1, α>0, β>0. (i, j) correspond to the trust value of node j for node i. $d(i,j)$is the direct trust value. $i(k,j)$ stands for the recommendations provided by node k that belongs to the neighbor set Cj of node j. n denotes the number of neighbors and l indicates the sequence number of the evaluation records and αandβ the weighed factors that are related with the security policies .Larger value for α denotes that the sensor node in WSNs is highly influenced about its own judgement. Similarly, a larger value for β signifies that the trust evaluation process is based on recommendations provided by other nodes are more trust worthy in trust evaluation process. In addition, the trust value is subject to 0≤t≤1. Generally, higher the trust value the sensor node , more trust worthy it is. The effect of conflicting behavior attacks can be minimized by setting adequate values ofαandβ, because the behavior of nodes can be viewed by its neighbors in the network, if a malicious node acts differently to different nodes, at that time it can be noticed by treating the combination of direct trust and indirect trust. The evaluation of direct trust is given by

$$dt(i,j)^l = \gamma_1 \times dt_{P(j)}(i,j)^{l-1} + \gamma_2 \times dt_{N(j)}(i,j)^{l-1} + ids(i,j)^l \quad (2)$$

Where $dt_{P(j)}(i,j)^{l-1}$ means the direct trust value of node $j$and for node i based on node j's past well-behaved behavior ,and $dt_{N(j)}(i,j)^{l-1}$ is the direct trust value of node j for node i based on node$j$'s past malicious behavior. γ1 and γ2, the exponential decay time factor that corresponds to the n positive and negative estimation, respectively. The assessment for current is denoted by$ids(i,j)^l$ by utilizing intrusion detection systems. The $ids(i,j)^1$ is given by

$$ids\ (i,j) = \begin{Bmatrix} P(j), for\ 0 < P(j) < 1 \\ 0, for\ uncertain \\ N(j), for -1 < N(j) < 0 \end{Bmatrix}$$

Where P(j) and $N(j)$ represent the positive and negative estimation for device j's behavior, respectively. These parameters should follow the rule that good reputation is highly complicated to gain than that of bad one. If the judgment for nodes' behavior is not absolutely sure, at that very time the value of $id(*)$should be set to zero.

The corresponding indirect trust evaluation process can be found by

$$\sum_{(K\in C_j, K\neq i)}^{n} it(k,j)^l = \sum_{(K\in C_j, K\neq i)}^{n} dt(i,k)^l \times dt(k,j)^l \quad (3)$$

In this model, we make use of the trust chain to compute the indirect trust of sensor nodes. $d(i, k)$ means for the direct trust value of node k for node i. The Direct trust value of node j for node that provides the recommendation data is represented by $dt(k, j)$. The highest product of all trust values determines the most trusted path, and thus the trust of path can be calculated by

$$t(p) = \Pi\ (\{\, t(i,j) \mid i,j \in p, i \longrightarrow j \,\}) \quad (4)$$

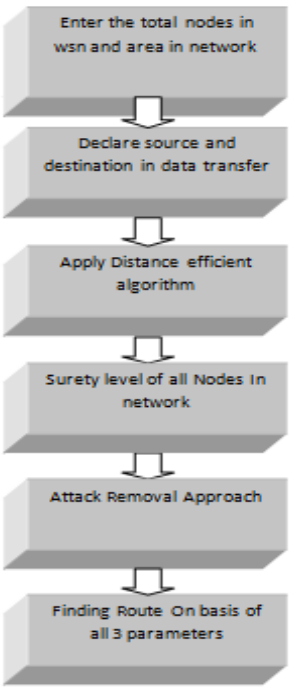
Where node i and node j are neighbors (J. Lopez, R. Roman, I. Agudo, and C . Fernandez Gago, 2010) , (J. Duan, D.Gao, C.H. Foh , and H.Zhang,2013), (Y. L. Sun, W. Yu, and Z. Han,2006).

2. Proposed

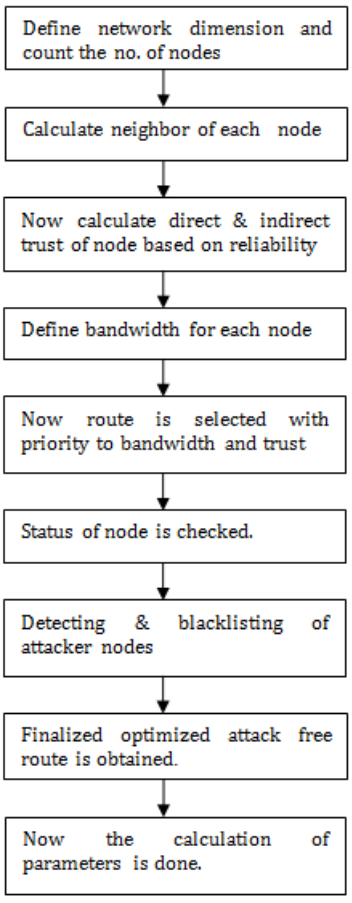
The main problem that we faced earlier was that only distance parameter is used but rest of QOS parameters are not used at all, so there is need to give some priority to those parameters to achieve for instance, higher throughput, utilize lesser energy etc. Many algorithms were developed but were not able to solve this problem. After studying them we have proposed a new protocol in which we have increased the QOS parameter in order to increase the throughput. The new parameter that we have introduced is Bandwidth. In our thesis the protocol that we are using will take both bandwidth and trust wise route selection in consideration .we will assign bandwidth to each node, then we will calculate threshold value of each node. In this the trust wise node is selected and the node with higher bandwidth is selected, and if both nodes are same then is taken as next node. If we select a node and if it satisfies both the condition i. e. it's most trustworthy and is having higher bandwidth than that node is taken as next node. If not then the next node is taken and this procedure is followed till we will get a route between source and destination.

Beside this the other problem was non prevention of attacker nodes. As the attacker node can be impeding the network to store incorrect routes, So in our thesis we have worked on these problems to find the better route between the source and destination .while finding the node from source it will first check whether the node is attacker node or not, if the selected node is an attacker node it will blacklist that node and that node will be removed from the network .After this it will

move to the next node and will follow the same procedure of finding the attacker node, if this node is not an attacker node it will take selected node in network and so on till the network is created or route is found .So in this way we have overcome these problem of routing in our thesis work.



Block diagram of Routing



3. Methodology

The methodology used in our paper is described in following steps:

1) Initially define a network dimension and count the nodes as to find the route between the source and destination.
2) After counting the number of nodes ,calculation of neighbors of each node is done
3) Calculate direct and indirect nodes on based on reliability. The node which is next to each node is taken as next node
4) In this step bandwidth is applied to every node that is present in the network dimension .As this is the parameter that is introduced so that we can increase the throughput.
5) Now a route is selected on the basis of bandwidth and reliability of each node .that is given in pervious step.
6) In this step the status of the selected node is node is attacker node checked, whether the node is malicious or not .
7) In this step the attacker node is detected, if it's an attacker node, blacklist that node This node will be removed from the route in the network ,and the next node will be checked by same procedure.
8) The above step is repeated till the route is found between source and destination. Finally an attack free route is obtained between the source and destination.
9) Finally after finding the route between source and destination, the calculation of parameters is done by checking fir its malicious behavior.

4. Results

Experimental results shows a selected route based on maximum trust and bandwidth while eliminating the malicious node. Thus, obtaining a constant packet delivery rate. Figure 1 and Figure 2 shows the network and predefined malicious nodes.

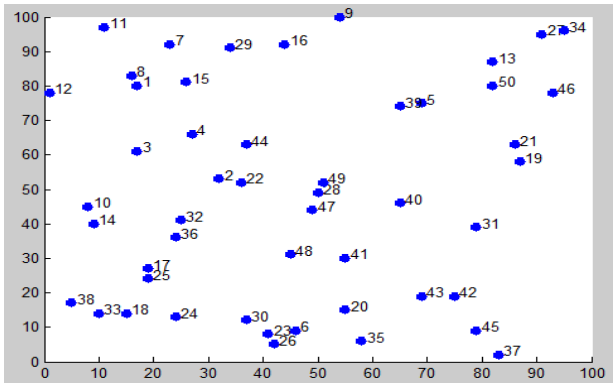


Figure 1: Defines the network

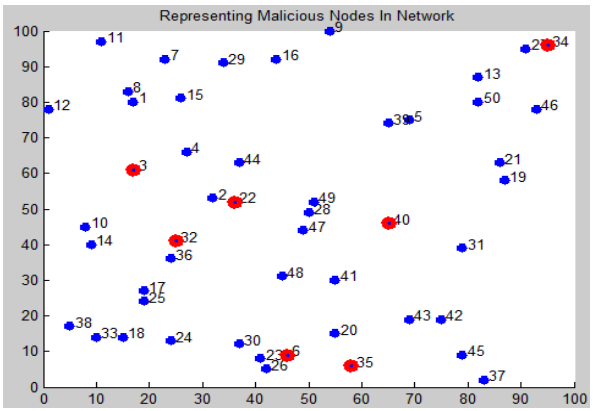


Figure 2: Represents mallicious nodes (RED)

Figure 3 shows the route including malicious node i.e. attacker nodes, Figure 4 indicates the route based on the best combination of trust and bandwidth , while eliminating the malicious or attacker nodes.

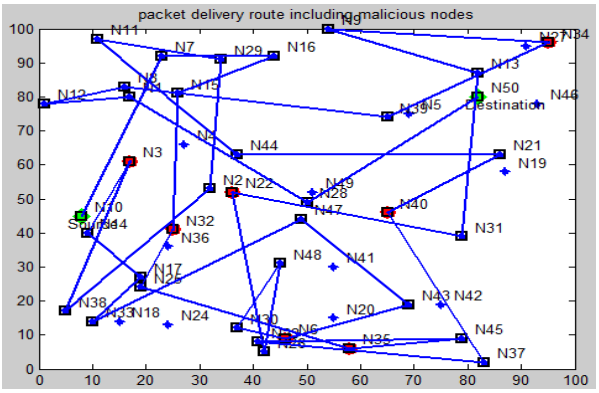


Figure 3: Defines route including mallicious nodes(RED)

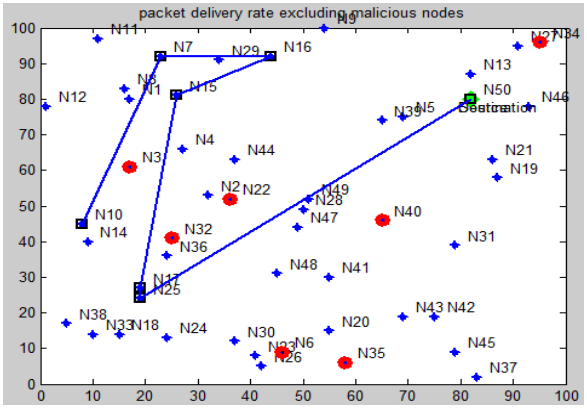


Figure 4: Route excluding mallicious nodes

Figure 5, 6, 7 and 8 show overall throughput (bandwidth), trust, distance and proposed packet delivery rate respectively Figure 9 shows packet delivery rate without bypassing malicious nodes. Finally figure 10 shows comparison of packet delivery rates

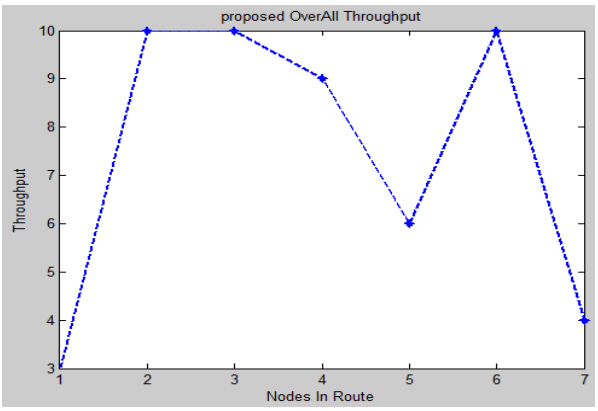


Figure 5: Proposed overall througput

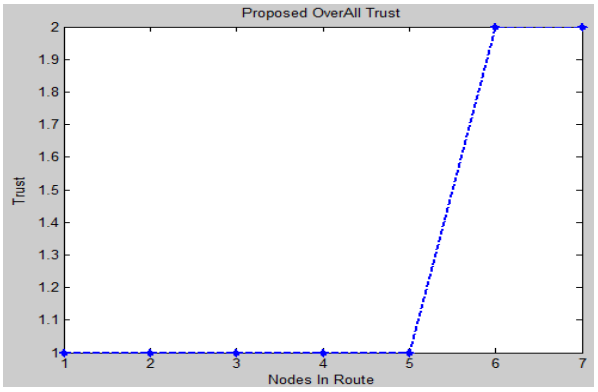


Figure 6: Proposed overall Trust

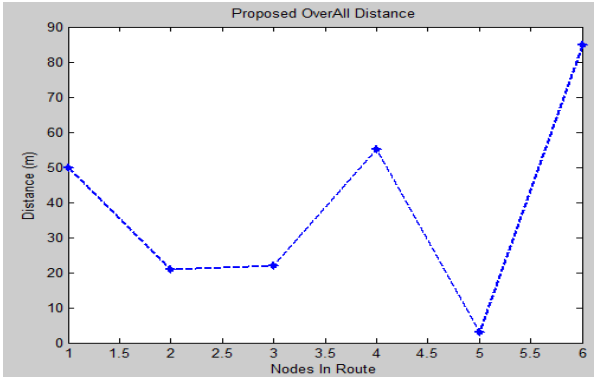


Figure 7: Proposed overall distance

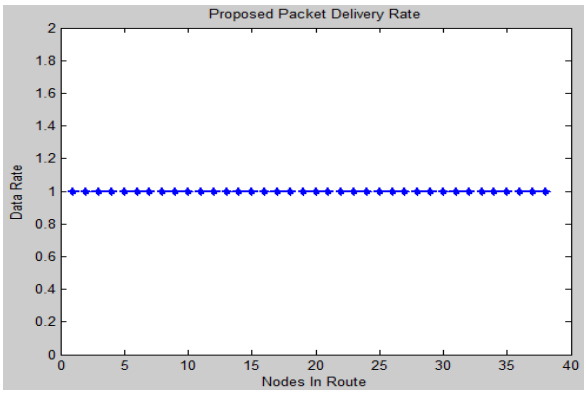


Figure 8: Proposed Packet Delivery rate

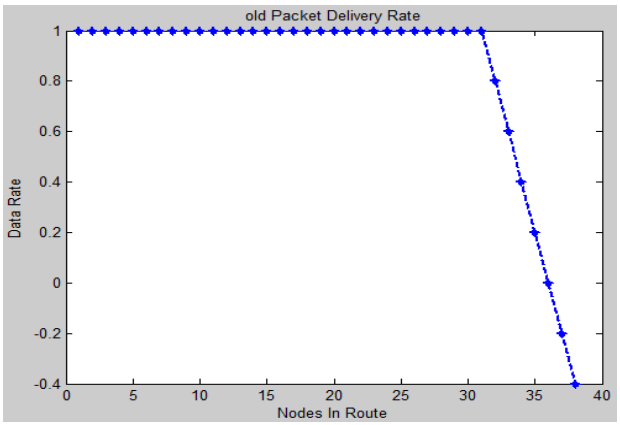


Figure 9: Old packet delivery rate

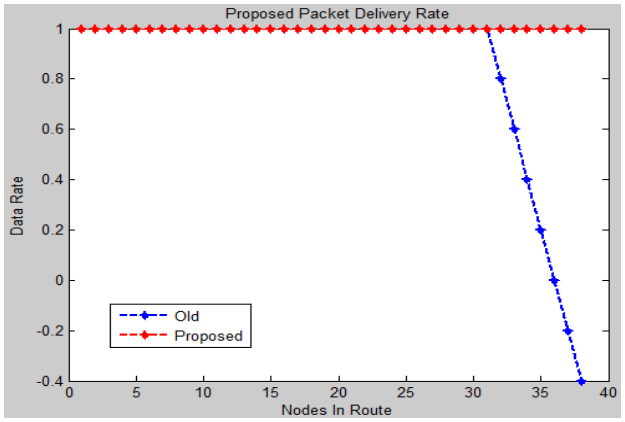


Figure 10: Comparison of proposed and old packet rates

Conclusion

In this paper we routed the packets based on trust calculations and other performance metrics, we utilized distance vector and the trust value of node to find the next node in the path from source to destination,in addition we introduced a parameter bandwith in our route selection to increase througput.further we identified the malicious nodes and these malicious nodes were dropped during routing process.in results it is clear that overall throughput increased and overall distance reduced and packet delivery rate remained constant.

References

Son, B., Her, Y., Kim, J., (September 2006), A Design and Implementation of Forest-Fires Surveillance System based on Wireless Sensor Networks for South Korea Mountains, IJCSNS International Journal of Computer Science and Network Security, vol.6 No.9B, 124–130.

Mainwaring *et al*,(Sep. 2002), Wireless Sensor Networks for Habitat Monitoring, International Workshop on Wireless Sensor Networks and Applications (ACM), ,

Chintalapudi, K.; Fu, T.; Paek, J.; Kothari, N.; Rangwala, S.; Caffrey, J.; Govindan, R.; Johnson, E.; Masri, S.,(March-April 2006), Monitoring civil structures with a wireless sensor network, Internet Computing, IEEE, vol.10, no.2, pp. 26-34,

Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury,(March 2007), A survey on wireless multimedia sensor networks, The International Journal of Computer and Telecommunications Networking, Vol. 51 , Iss. 4, , pp. 921-960.

V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi,(2008) Security in wireless sensor networks, Wirel. Commun. Mob. Comput. 8:1–24.

T.Kavitha, D.Sridharan,(2010), Security Vulnerabilities In Wireless Sensor Networks: A Survey Journal of Information Assurance and Security, Vol. 5031-044.

Jaydip Sen, (August 2009), A Survey on Wireless Sensor Network Security, International Journal of Communication Networks and Information Security (IJCNIS)Vol. 1, No. 2,.

B. C. Villaverde, S. Rea, and D. Pesch,(2012), InRout—a QoS awareroute selection algorithm for industrial wireless sensor networks,Ad Hoc Networks, vol. 10, no. 3, pp. 458–478,.

D. A. Tran and H. Raghavendra,(2006), Congestion adaptive routingin mobile ad hoc networks,IEEE Transactions on Parallel andDistributed Systems, vol. 17, no. 11, pp. 1294–1305,.

M. L. Das,(2009), Two-factor user authentication in wireless sensornetworks,IEEE Transactions on Wireless Communications,vol.8, no. 3, pp. 1086–1090,

G. Zhan, W. Shi, and J. Deng, (2012),Design and implementationof TARF: a trust-aware routing framework for WSNs,IEEETransactions on Dependable and Secure Computing,vol.9,no.2, pp. 184–197,

S. Marti, T. J. Giuli, K. Lai, and M. Baker, (August 2000),. Mitigating routingmisbehavior in mobile ad hoc networks, inProceedings of the6th Annual International Conference on Mobile Computing andNetworking (MOBICOM '00), pp. 255–265, ACM,

J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago,(2010), Trustmanagement systems for wireless sensor networks: best practices, Computer Communications, vol.33,no.9,pp.1086–1093.

J.Duan,D.Gao,C.H.Foh,andH.Zhang,(2013),TCBAC:atrustandcentrality degree based access control model in wireless sensornetworks,Ad Hoc Networks,vol.11,no.8,pp.2675–2692,.

Y. L. Sun, W. Yu, and Z. Han,(2006), Information theoretic frameworkof trust modeling and evaluation for ad hoc networks,IEEEJournal on Selected Areas in Communications,vol.24,no.2,pp.305–315,.