Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 373 – 380

Procedia Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

QoS Aware Trust Metric based Framework for Wireless Sensor Networks

Prabha R[1], Krishnaveni M[1], S H Manjula[1], K R Venugopal[1], L M Patnaik[2]

[1]*University Visvesvaraya College of Engineering ,Bangalore 560056, India*

[2]*Indian Institute of Science, Bangalore 560 001, India*

Abstract

Wireless Sensor Networks have gained popularity due to their real time applications and low-cost nature. These networks provide solutions to scenarios that are critical, complicated and sensitive like military fields, habitat monitoring, and disaster management. The nodes in wireless sensor networks are highly resource constrained. Routing protocols are designed to make efficient utilization of the available resources in communicating a message from source to destination. In addition to the resource management, the trustworthiness of neighboring nodes or forwarding nodes and the energy level of the nodes to keep the network alive for longer duration is to be considered. This paper proposes a QoS Aware Trust Metric based Framework for Wireless Sensor Networks. The proposed framework safeguards a wireless sensor network from intruders by considering the trustworthiness of the forwarder node at every stage of multi-hop routing. Increases network lifetime by considering the energy level of the node, prevents the adversary from tracing the route from source to destination by providing path variation. The framework is built on NS2 Simulator. Experimental results show that the framework provides energy balance through establishment of trustworthy paths from the source to the destination.

Keywords: **Energy Awareness, Routing Security, Trustworthiness, Quality of Service, Wireless Sensor Networks**

Prabha R. Tel.: +91 9731599240 *E-mail address: heshakil@yahoo.com*

doi:10.1016/j.procs.2015.04.196

1. Introduction

Efficient solutions for a great variety of applications can be built based on a set of low-cost sensors organized in a wireless network. The potential application domains include military fields, healthcare, homeland security, industry control, intelligent green aircrafts and traffic control in smart roads. Although networking and security technologies are in an advanced stage, wireless sensor networks present intricacies which dictate the design of new protocols. First, these networks operate in an infrastructure-less adhoc manner, which implies that the communication relies on the cooperation among nodes for the accomplishment of basic networking tasks such as routing. Each time a sensor needs to send the sensed value to the data sink, it looks for an available neighbour. As these are ad hoc networks which operates in a self-organized manner, a malicious node may enter the network. Due to the wireless operation, eavesdropping can be easily performed in this environment which makes the network vulnerable not only to privacy attacks, but also to traffic analysis attacks which threaten the whole network operation.

Network layer in Wireless Sensor Networks (WSN) is the target of many types of attacks. As an instance, in black hole attack, adversary nodes do not forward the packets completely. In case of grayhole attack few packets are forwarded selectively. While in Sybil attack a node exhibits multiple identities. These kinds of nodes can exist in different neighbourhood and results in more packet dropping. Wormhole attack is a kind of attack, where an understanding between the two adversary nodes is written to introduce other attacks in the network like black hole attack. In case of wormholes adversary misguides a received packet and sends it to its neighbours by adding fake routing decisions. In order to prevent the WSN form the different types of attacks trust evaluation among the nodes is a must and it is the one of the critical part of any WSN. Trust varies with time, trust value of a node increases or decreases with time. Trust valve of a node is a mathematical representation of nodes attitude of another node in the network. Mathematical tools are used to represent trust and reputation of a node in the network. A record of transactions among the neighbours is maintained, to establish a trust value of a node.

2. Motivation and Contribution

Providing the network level privacy in wireless sensor networks is sub divided into four types- (i) identity (ii) route (iii) location and (iv) data privacy. Due to the existing constraints in the WSN achieving network level privacy is a challenging task. QoS Routing Protocols and Privacy in Wireless Sensor Networks [1] algorithms employ a routing pattern that does not cater to trustworthiness in presence of energy constraints and attacks. The existing privacy protection schemes are unable to provide privacies of different types-identity, route, location and data privacy. The main contribution of this paper is design and implementation of Trust Aware Routing (TAR) Algorithm to achieve network level security. TAR algorithm secures the WSN form any intruders trying to access information form the network. TAR algorithm implements identity, route, location and data privacy to safeguard the WSN from an adversary misdirecting the multi-hop routing and security attacks.

3. Organization

Section 4 discusses the Related Work, Section 5 states Problem Definition, Section 6 explains the TAR Algorithm, Section 7 presents the Performance Analysis followed by Conclusion and References.

4. Related Work

Wireless sensor networks are often deployed in a hostile environment and work without human supervision, individual node could be easily compromised by the adversary due to the constraints such as battery lifetime, smaller memory space and limited computing capability. Security in WSN has been one of the most important topics in the WSN research community. Here we briefly review the reported works closely related to malicious node detection. Junqi *et al.*,[2] presented a trust establishment and Management frame work for hierarchical wireless sensor networks. The proposed frame work helps to minimize the memory, computation and communication overhead involved in trust management in wireless sensor networks. Idris *et al.*, [3] proposed a novel scheme based on weighted-trust evaluation to detect malicious nodes. The hierarchical network can reduce the communication overhead between sensor nodes by utilizing clustered topology. In [4] a novel algorithm based on Weighted Trust Evaluation to detect malicious nodes for hierarchical sensor networks is proposed in this paper. The hierarchical network can reduce the communication overhead among sensor nodes by utilizing clustered topology. The proposed algorithm models a cluster of sensor networks and detects malicious nodes by examining their weights that represent the reliability of sensor nodes. Theodore *et al.*, [5] developed a trust-aware, location-based routing protocol which protects the WSN against routing attacks. The protocol provides a solution for detection and avoidance of malicious nodes in the network.

Nomenclature

N	Number of Nodes in the Network
T	Number of Trusted Nodes in the Network
M(t)	Set of Trusted Nodes in the Network
M(tF)	Forward Neighbour set of a Node
M(tRb)	Right Backward Neighbour set of a Node
M(tLb	Left Backward Neighbour set of a Node
M(tMb)	Middle Backward Neighbour set of a Node
nexthop(k)	Chosen Next Hop of a Node k
Contention(x)	Random Node Selection from the Set x
$\text{Energy}_{\text{critical}}$	Threshold Energy of a Node to participate in Communication
Energy(k)	Energy of node k

5. Problem Definition

The main objective of our TAR algorithm is to achieve full Network Level Privacy consisting of Identity, Route, Location and Data privacy. TAR secures the multi-hop routing in wireless sensor networks against intruders by evaluating the trustworthiness of neighbouring nodes. A node is considered trustworthy if it interacts successfully most of the time with the other nodes. A node is considered untrustworthy if it tries to do as many unsuccessful interactions as possible with the other nodes.

Table 1 : Algorithm for Trust Aware Routing (TAR) in WSN

```
Input : trust worthy neighbouring node set for all the nodes
Output: energy efficient variable path for reliable transmission
Step 2: if $M(tF)$ is not null then
Step 3:     nexthop ( $k$ ) = Contention( $M(tF)$ );
Step 4:     if $Energy_{critical} < (Energy(k) - Energy_{transmission})$ and
              $Energy_{critical} < (Energy(nexthop(k)) - Energy_{reception})$ then
Step 5:       Selected next hop is used to transmit the packet to the destination
                 $Energy(k) = Energy(k) - Energy_{transmission}$
               $Energy(nexthop(k)) = Energy(nexthop(k)) - Energy_{reception})$
Step 6:     else go to step 2 with $M(tF) = M(tF) - nexthop(k)$
Step 8:      end if
Step 9: else if $M(tRb) \cup M(tLb)$ is not null then
Step 11:     nexthop( $k$ ) = Contention$( M(tRb) \cup M(tLb));$
Step 12:     if $Energy_{critical} < (Energy(k) - Energy_{transmission})$ and
             $Energy_{critical} < (Energy(nexthop(k)) - Energy_{reception})$ then
Step 13:    Selected next hop is used to transmit the packet to the destination
                        $Energy(k) = Energy(k) - Energy_{transmission}$
                        $Energy(nexthop(k)) = Energy(nexthop(k)) - Energy_{reception})$
Step 14:     else
Step 15:     go to step 11 with $M(tRb) \cup M(tLb) = (M(tRb) \cup M(tLb)) - nexthop(k)$
Step 16:     end if
Step 17: else if $M(tMb)$ is not null then
Step 18:     nexthop($k$) = Contention($M(tMb$
Step 19:     if $Energy_{critical} < (Energy(k) - Energy_{transmission})$ and $Energy_{critical} < (Energy(nexthop(k)) - Energy_{reception})$ then
Step 20:    Selected next hop is used to transmit the packet to the destination
                        $Energy(k) = Energy(k) - Energy_{transmission}$
                        $Energy(nexthop(k)) = Energy(nexthop(k)) - Energy_{reception})$
Step 21:     else
Step 22:     go to step 17 with M(tMb) = M(tMb) – nexthop(k)
Step 23:     end if
Step 24: else
Step 25: Drop packet and Exit;
Step 26: end if
Step 27: end if
```

6. Algorithm

This section explains Trust Aware Routing algorithm for wireless sensor network. TAR algorithm is a distributed trust model which depends on trust information of neighbouring nodes in order to safeguard the WSN from routing and trust related attacks. In TAR a distributed trust management framework is implemented in order to measure the reliability of the nodes which is given in table 1.

In the initialization phase of the network , trust based classification of nodes is done and neighbour node sets are initialized for every node. In the routing phase the TAR algorithm is called. TAR forwards the packet, by first checking the availability of the trusted neighbouring nodes in its forward direction set $M(tF)$. If trusted nodes exists then it will randomly select one node as a next hop from the set $M(tF)$. In addition interrogation of energy level of the sending and receiving nodes is carried out. If there is a node with the defined constraints, that node becomes the forwarder node. If no trusted node is available in its forward direction i.e $M(tF)$, then the source node will check the availability of a trusted node in the right ($M(tRb)$) and left ($M(tLb)$) backward sets. If the trusted nodes are available with satisfying energy constraints, then the source node will randomly select one node as a next hop from these sets and forward the packet towards it. If such a node does not exist in these sets either, then the source node will randomly select one trusted node from the backward middle set ($M(tBm)$) and forward the packet towards it with energy criterion taken into consideration. In all these cases if a random node selected does not meet the energy constraints, the chosen set is iterated until it exhausts. If TAR is unable to find a trusted node among all the available neighbour sets then the packet is simply dropped.

Table 2: Simulation Parameters used in the simulation

Parameters	Value
Network Architecture	Homogenous Flat
Area Size	500 m x 500 m
Number of nodes	20,40,50,100
Deployment Type	Random
Transmission range	250 m
Initial Energy	1000 mj
Mac Layer	Mac/802.11
InterfacequeueType	Queue/DropTail/PriQueue
Link Layer Type	LL
Least Utilization Time	0.1 seconds
Maximum Utilization Time	10 seconds
Application Type	Event Driven

6. Performance Analysis

This section gives the details of performance analysis of our QoS Aware Trust Metric based Algorithm Implemented on NS2 Simulator [7].

6.1 Simulation Set up

The simulation is carried out using NS2 simulator. The deployment parameters and the network parameters used in the simulation is summarized in Table 2

6.2 Results

The QoS performance Metrics considered for analysis of the TAR algorithm are: (i) Average Energy: The energy consumption for the transmission of a packet from source to destination is basically dependent on the number of the intermediate hops taken in that route. As the number of hops increase in that route, proportionally energy consumption increases. From simulation time 1 to 3, the energy consumed increases sharply because of the energy being utilized for flooding of the hello packets at the initialization phase and routing table information related querying. Once the routing phase starts, the energy is dependent on the path chosen (number of intermediate hops). The energy consumed increases gradually after that depending on the path length and then saturates at some point as the complete route from source to destination involves same number of intermediate nodes. When there is normal transmission (attack- free), the total energy consumed is equal to the sum of the energy consumed for single hop transmissions for the intermediate hops. When there is attack-prone transmission there is retransmission involved because of lack of acknowledgement in time. Retransmissions add up energy consumption, thus it can be seen from the figure 2 that with attack energy consumption is more as compared to its counterpart-without attack. From the approach that we have used, the communication is not attack prone since all the nodes involved in the communication are trust worthy hence the curve depicts less energy consumption.

ii) Throughput: Throughput refers to number of packets received per unit time. In case of throughput without attack, the number of packets reaching the destination from the source will be very low initially due to the initial setup (neighbor node classification and trust evaluation). Once the path is established between the source and destination, the packets flow in the designated path up to the link/ channel capacity which is shown with the curve for throughput with no attack. This saturates at the point of link capacity. In case of attacks, the throughput will be less because additional re-transmissions make the number of packets reaching the destination low in number. The re-transmission event occurs at simulation time 2 and involves increment thereafter. However it is not able to cross its counterpart because of the chain of re-transmissions occurring at various intermediate nodes. In case of transmission with attack, the number of packets received per unit time will be lesser than that of the number of packets received without attack hence the throughput is less .

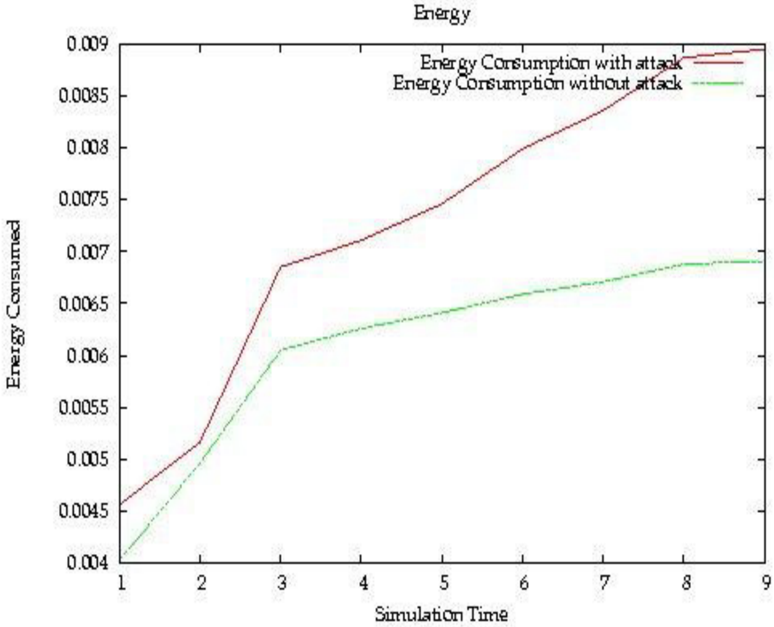

Figure 2: Simulation Time versus Energy Consumed

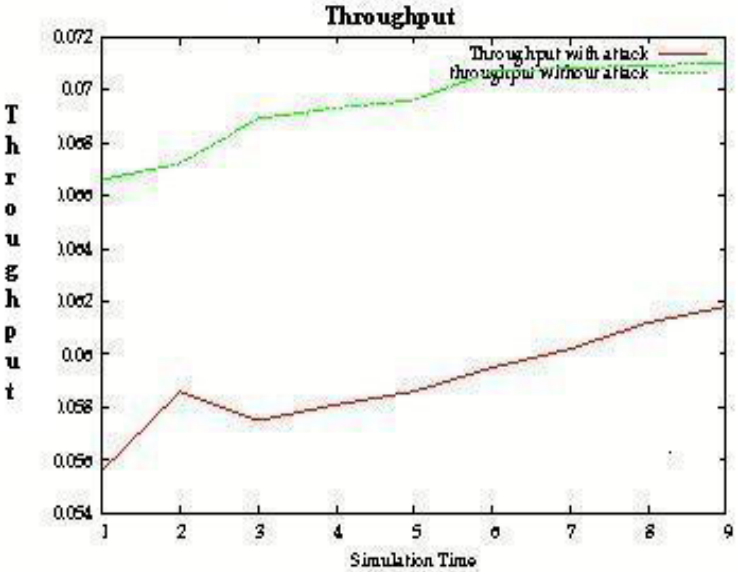

Figure 3 : Simulation Time versus Throughput

7. Conclusions

This paper proposed the TAR algorithm that is trustworthy thereby providing security against WSN attacks. The algorithm works on the concept of randomness in direction meaning to say that the neighbours are classified based on their direction property and randomness is involved in selecting the next hop in transmission. Because of this direction property and randomness, there is path variation and path length variation for the same set of source and destination. The algorithm is simulated using NS2 simulator. The QoS Routing performance namely throughput of TAR is determined and also compared with simulated attack by varying the malicious nodes from 20, 30,40 and 100 nodes with coverage area of 500×500 m2.

References

1. Phani Praveen and Sukumar Babu .“ Qos Routing Protocols and Privacy in Wireless Sensor Networks”, *Global Journal of Computer Science and Technology*, vol. 12, no. 4, 2012.
2. Junqi Zhang, , Rajan Shankaran, , Mehmet A Orgun,, Vijay Varadharajan and Abdul Sattar,” A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks”, *International Conference on Embedded and Ubiquitous Computing,* 2010.
3. Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su,” Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation”, *The Symposium on Simulation of Systems Security (SSSS'08)*, Ottawa, Canada, April 14 –17, 2008.
4. Hongbing Hu, Yu Chen, Wei-Shinn Ku , Zhou Su and Chung-Han J. Chen “Weighted Trust Evaluation-based Malicious Node Detection for Wireless Sensor Networks” *International Journal of Information and Computer Security*, vol. 3, no. 2, 2009.
5. Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas, Ioannis Papaefstathiou , Charalambos Vangelatos and Lionel Besson, “Trust Aware Routing Protocol for Large Scale WSN's”, *International Journal of Network Security and Its Applications*, vol. 2, no.3, July 2010.
6. Laura Gheorghe, Razvan Rughini and Nicolae Tapus,” Trust and Energy-aware Routing Protocol for Wireless Sensor Networks”, *The Eighth International Conference on Wireless and Mobile Communications,* 2012.
7. NS2 Simulator Site: http:// www.isi.edu/nsmam/ns.