IDENTIFYING TRUSTED ROUTING PATH IN WSNS THROUGH TARF

S.ANITHA,
II YEAR, M.E (COMMUNICATION SYSTEM),
PGP COLLEGE OF ENGINEERING AND TECHNOLOGY,
NAMAKKAL.

Mrs.A.NITHYA,
Asst.Professor,
PGP COLLEGE OF ENGINEERING AND TECHNOLOGY,
NAMAKKAL

Abstract— The multi-hop routing in wireless sensor networks (WSNs) will provide little safe against identity deception through replaying routing information. This may be create various dangerous attacks against routing information, attacks such as Sinkhole attacks, Wormhole attacks and Sybil attacks. These types of attacks cannot completely remove from network through our traditional cryptographic technique. In order to secure wireless sensor networks from various attacks through misdirecting multihop routing, I have design and implement TARF, for dynamic WSNs,a robust trust aware routing framework is used .This trust aware routing framework does not depends upon the accurate time synchronization or distribution of nodes within the sensor network. This TARF will provide trust worthy and energy efficient routing path in wireless sensor network. Mostly TARF proves effective against those harmful attacks developed because of identity deception through replaying routing information. Further, I implement a TARF in TinyOS, and verified through Network Simulator.

1 INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring. A Wireless Sensor Networks (WSN) contains hundreds or thousands of sensor nodes, so each sensor nodes are getting power via battery. Since sensor node will do limited processing only. In a narrow radio communication range, each sensor node with in wireless sensor networks will wirelessly transmit messages to a base station via a multi-hop path.

This multi-hop routing of WSNs will provide target of various types of attacks such as Sinkhole attack, Wormhole attack and Sybil attack. An attacker may destroy nodes physically, create collision on traffic, drop or misdirect the communication in routes or block the communication medium. My work concentrates on the kind of attacks in which intruders misdirect network through replaying routing information. Depending on identity deception, the intruders are eligible for launching harmful attacks such as Selective forwarding, Wormhole attack, Sinkhole attack and Sybil attack. In a Wormhole attack, the attacker node will get the data at one part of the network and tunnel that packet and put it in the some other part of the network, that network is not participate in current network. In a Sinkhole attack ,Sink means ‘destination’, an attacker node may be claim it’s to be a original base station, but original base station is far away from this fake base station. In Sybil attack, a single node contains identity of multiple nodes, if there is any attack on that node means multiple nodes are getting affected. All those attacks are occurred in wireless sensor network because of replaying routing information. It is very difficult for identifying attacker node and honest node with in a poor network connection. The existing routing protocol of wireless sensor networks (WSN) consider only honesty of nodes and focus on energy efficiency, but it fails for protecting WSNs from unauthorized participation by authentication and encryption. Example of authentication and encryption schemes for WSNs includes Tinysec, Spins, Tinypk, and TinyECC. In WSNs will get the each sensor node will get the power through battery. So it is very difficult for incorporate security as one of the most important things in WSNs if perfect encryption and authentication is used in WSNs, attacker node still present in the network because of replaying routing information.

The Gossiping based routing protocols provides little protection against by selecting random neighbors to forward packets. The disadvantages of Gossiping based routing protocol is waste of energy. Since it will choose random neighbors, that random neighbor may be honest node or attacker node, if it is attacker node means it does not forward the packets which is send by source node, hence it does not provide energy efficiency. Another existing routing protocol is cryptographic method along with trust and reputation management scheme applied in WSNs for providing secure routing protocol. The trust and reputation management will assign trust value for each sensor node based on past performance of their routing function. Based on that trust value, the secure and efficient routing path is selected. The main drawback of this method is, it does not provide better performance in WSNs, since WSNs is resource constrained. All existing routing protocol of WSNs mainly depends on the accurate time synchronization and distribution of nodes with in the wireless sensor networks (WSN) that is called as geographic information. At this point, to protect WSNs from various types of attack, I have design and implement a robust trust aware routing framework, TARF, in order to secure a wireless sensor networks (WSN).This technique can be implemented in WSNs even though its resource constrained, and also this technique will allow full flexibility for incorporate with existing routing protocol. A trust aware routing protocol will provide better network performance if Sinkhole attack, Sybil attack, Wormhole attack are present in the network. The main advantages of this proposed technique is, it does not depend on the tight time synchronization and geographic information.

2 DESIGN PRINCIPLES

In data collection task of WSNs, each sensor node will send the data to base station through some intermediate node. This is called as multihop routing function of WSNs.It is shown in Figure 1.An intruders may cheated the identity of any honest node through responding that node's outgoing routing packets and spoofing their acknowledgement.

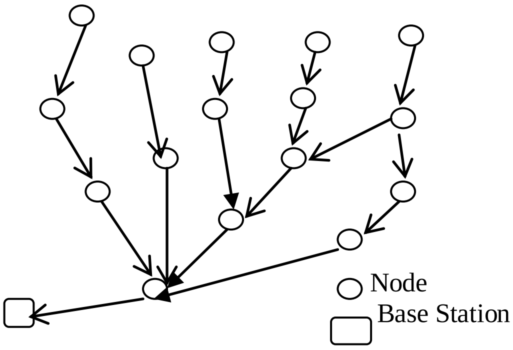

Fig 1.Multi-hop routing function

This multihop routing can be applied to cluster based WSNs.In cluster based WSNs data are collected by clusters before being transmitted. The main advantage of this approach is energy saving and efficient bandwidth utilization.

2.1 Authentication requirements

The main requirement of TARF is the transmitted packets are properly authenticated. Importantly broadcast message from base station about data delivery must be authenticated. If broadcast message from base station is asymmetrically authenticated, it's very difficult for intruders to forge a broadcast message from base station. Especially with authenticated broadcast, even with presence of attackers, TARF may use TrustManager to choose trustworthy path. The asymmetric authentication of broadcast packets from base station is used for providing secure routing protocol. This asymmetric authentication is achieved by using technique called µTESLA.The packet other than broadcast message from base station is authenticated by symmetric authentication technique. This symmetric authentication operation is performed by using technique called Tinysec.

2.2 OBJECTIVES

TARF mainly protect a WNSs against attacks misdirecting the multihop routing, especially those attackers are existing because of replaying routing information. The main aim of TARF as follows,

High Throughput

Throughput is defined as ratio of the number of all data packets are delivered to base station to the number of sampled data packets. Throughput defines how efficiently the network is collecting and delivering data to base station.

Energy Efficiency

Data transmission is most part of energy consumption. The energy efficiency is defined as average energy cost to successfully deliver a unit sized data packet from source node to the destination node that is base station. The energy efficiency can be calculated by using hop per delivery. Evaluation of energy efficiency is depends on number of one hop transmission is occurring.

3 TARF DESIGN

By evaluating trust value of neighboring nodes, TARF secure the multihop routing in WSNs against attacker misdirecting the routing path. TARF determine such a attacker by their low trust values. The main benefit of TARF is energy efficient, high scalable. There are several notations are used in TRAF, they are

Neighbor

For a node N, neighboring node of N is reachable from N with one hop wireless transmission.

Trust level

Trust level of neighbor is determined by how neighbor node correctly delivers data received to the base station.

Energy cost

For a node N, the energy cost of a neighbor is the average energy cost for successfully deliver a unit sized data packet from current node to next hop node.

3.1 Overview

For TARF enabled node N will route a data packet to the base station based on which neighbor will have high trust value and energy efficiency. Once data is forwarded to that node, the remaining work to deliver a data packet to base station is carried out by that node.TARF enabled node maintains a neighborhood table with trust level value and energy cost values for certain neighbors which is known to that node. In TARF, there are two type of routing information is exchanged in addition to data transmission. Broadcast message from base station about data delivery and energy cost report message from each node. Both messages does not need acknowledgement. The broadcast message from base station about data delivery is broadcast to whole network. This message is identified by suitable node through source sequence field. Another type of message exchanged is energy cost report message from each node. That message only broadcast to neighbor node if any nodes receive the energy cost report message it will not forward to next node. For each node in WSN, to maintain neighborhood table with trust values and energy cost value of neighboring node. Two components are required for TRAF. They are Trust Manager and Energy watcher. Energy Watcher will record the energy cost for each known neighbor based on continuous monitoring of the one hop transmission from that node to immediate neighbor of the node and that neighbors will send the energy cost report message to that particular source node. The attacker node may be sending falsely energy cost report in that source node in order to select it's as a neighboring node. This problem can be overcome by TARF through it will choose neighboring node based on both energy cost value and trust value of that node. The TARF enabled neighboring node will eliminate attacker node by using low trustworthiness of that node. It can be performed by a component called as Trust Manager.

Trust Manager will assign trust value for each neighbor based on creation of network loop and broadcast message from destination about its delivery of packet. Once node will decide its next hop neighbor by using neighborhood table, that next hop neighboring node will send energy cost report message. This message is flooded to all its neighbors to indicate energy cost required to transmit a data from the node to the base station. Each node in WSNs will select next hop node based on neighborhood table. In order to maintain a neighborhood table two components run on each node, such as Trust Manager and Energy Watcher. The function of Energy Watcher and Trust Manager is explained in following figure.

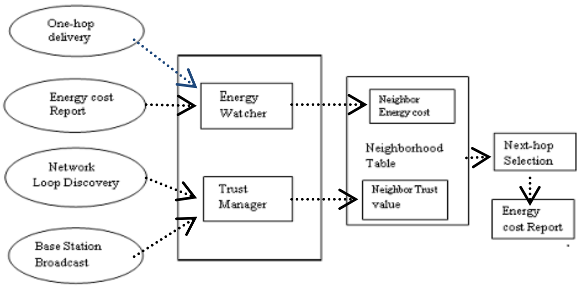

Fig 2.TARF Design

3.2 Routing Procedures

In WSNs, the source node will send detected event of interest to base station through some intermediate nodes. This is the function of multihop routing. In order to maintain stability in routing path, TARF enabled node will maintain same next hop until next new broadcast message from the base station is occurred. At the same time to reduce the traffic in network, their energy cost reports of that next hop node do not occur until broadcast from base station is changed. If a TARF enabled node does not choose next hop node until next new broadcast message from base station, it will provide guarantee for all path as a loop free path.TARF enabled node will change their next hop node when their chosen next hop node will receive and deliver data properly.

3.2.1 Selection of routing path

Each node in WSNs will select the next hop node based on their neighborhood table by considering energy cost and trust value of that node. The TARF enabled node will eliminate attacker node that misdirect traffic by replaying routing information. For node N in WSNs will select the route for sending data to destination such as base station with optimal next hop node from that neighboring node by considering trust level and energy cost and finally forwarded the data to chosen next hop node immediately. If neighbors will have trust value below threshold value means, which neighbors will be excluded from the WSNs.Among the remaining neighboring nodes will select next hop node through by evaluating their energy consumption and reliability for successful delivery of packets. Therefore TARF enabled node will select next hop node with high trust values, it's automatically protects the network from an attacker who forges the identity of an attractive node such as base station. The energy driven route is achieved when each node in WSNs will choose their neighbors in terms of energy.

3.3 Energy Watcher

The main responsibility of Energy Watcher is, it will assign energy cost value for each node based on their one hop delivery of unit sized data packet to their neighbor and energy cost report message from that neighbor. There are several notations used in Energy watcher descriptions. The notations E_{Nb} denotes a average cost of successfully deliver a unit sized data packet from N to the base station, where b as N's next hop node and it is the responsible for remaining routing path. Here one hop retransmission may be occur until acknowledge received from their neighbor. This one hop retransmission cost also included in the calculation of average energy cost $E_{Nb.}$If suppose node N will select A as a next hop neighbor after comparing energy cost and trust level. Then the N's energy cost is E_N=E_{NA}.The $E_{N\rightarrow b}$ denotes as the average energy cost required for successful delivery of unit sized data pocket from node N to the next hop neighbor node as b with one hop transmission. Here it is very important to consider the retransmission cost also. From above notations it is very easy to establish a relation as E_{Nb}=$E_{N\rightarrow b}$+E_b.

3.4 Trust Manager

Trust Manager will assign trust value for each neighbor based on creation of network loop and broadcast message from base station about data delivery. For a Node N in WSNs, each neighbor b of N, Trust level value for neighbor b of N is denoted by T_{Nb} in neighborhood table. At the first, each neighbor node will have constant trust value as 0.5, if neighbor node will transmit their received data to next hop node means their trust value will be updated from their trust values. The trust manager mainly depends on the broadcast message from about data delivery. Trust Manager N on compares N's stored trust value of neighborhood table. This comparison is performed by based on delivery ratio. This is defined as ratio of the number of successfully delivered packets which are forwarded by this node to the number of those forwarded data packets.

3.5 Analysis of Trust Manager and Energy Watcher

Each node N in WSNs mainly depends on the Energy Watcher and Trust Manager in order to select efficient neighbor as its next hop node. There is a chance for compromised node to send the false energy cost report. This can be overcome by using Trust Manager. The main aim of attacker node is preventing data delivery rather than forwarding data packet in low efficient routing path.TARF will eliminate this problem through Trust Manager. Trust Manager on one node does not depends on the Trust Manager of the another node. If an attacker try to send false energy cost report message in order to form false routing path, this problem can be overcome by Trust Manager. When Trust Manager on node identifies many delivery failures from broadcast message from base station, it starts to degrade the trust level of that node. If their trust values goes below certain threshold it makes node to switch to another next hop node. The Trust Manager will degrade the trust value of honest next hop node when attacker node present after that next hop node. Trust Manager will improve the data delivery ratio by mitigating the attackes.It is very difficult for identifying attacker node in the network. Trust Manager will provide support for a node to choose another routing path when current routing path frequently fails to deliver a data to base station. The working function of Trust Manager is explained in following figure.

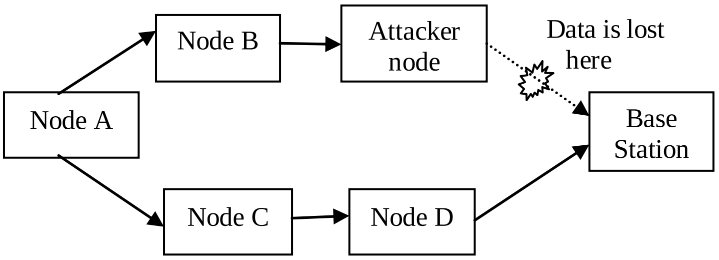

Fig 3.Trust Manager Function

In above figure node A, B, C, D is honest node not an attacker node. Node A has next hop node as node B, similarly node B has attacker node as its next hop node. This attacker node will drop whatever packet send by node B.So it makes data packet send by node B will not deliver at base station. Finally node A will identifies that the data packets it forwarded did not get delivered. The Trust Manager on node A will starts to decrease the trust level of its next hop node B even though node B is absolutely honest node. If trust level of that node is below the threshold value means, node A will select node C as its next hop node. By this way node A finally find a successful routing path as A-C-D-base station. If a valid node identifies trust worthy honest neighbor as its next hop node, it will maintain that next hop node until fake base stations occur in routing path. The main benefit of TARF is, it can be easily incorporate into existing routing protocol. The existing routing protocols are collection tree routing protocol (CTP) and Link connectivity protocol. The CTP protocol is much efficient and reliable. It analyses link quality in network for choosing the efficient next hop node.

4 CONCLUSIONS

I have designed and implemented TARF, a Trust Aware Routing Framework for WSNs, to provide security for multi-hop routing in WSNs against harmful attacker arising because of replay of routing information. Thus the implemented TARF provide trustworthiness and energy efficient routing path, which are play major role in hostile environment. By the concept of trust management, TARF enables node to monitor the trust value of its neighbor and thus to select reliable routing path. The main contribution of my work is listed below. First when comparing existing routing protocol for WSNs, TARF efficiently protects the WSNs from severe attacks such as Wormhole attack, Sinkhole attack and Sybil attack. Those attacks are occurred in network because of replaying their routing information. The main advantages of this proposed system was, it does not require time synchronization and distribution of nodes within the network.

While forwarding 220 packets, 99 packets are reached in Base Station. So TARF provide better Quality of Service (QOS) with acceptable Delivery ratio. The Quality of Service provided by TARF was explained in following figure.

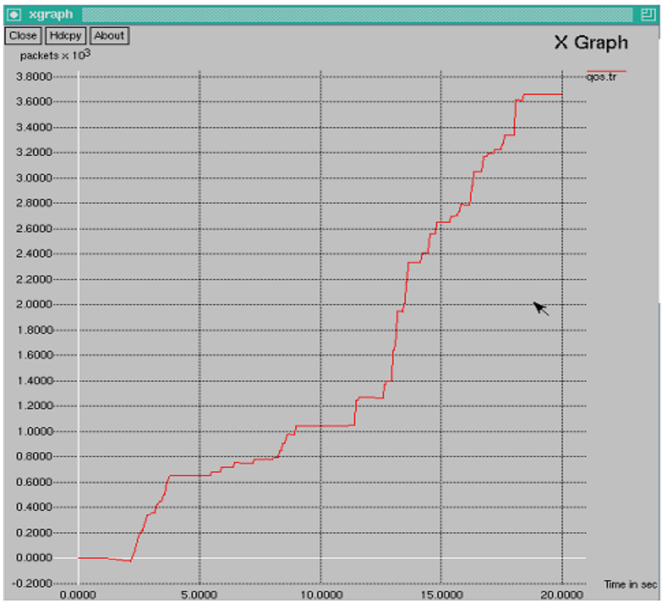

Fig 4.QOS of TARF

The TARF provide better energy consumption .Usually Energy was measured in Joules. The existing method was provided energy consumption value as 0.2joules.But this proposed system was proved energy consumption value as 0.5 joules. The energy consumption plot of TARF was shown in the following figure.

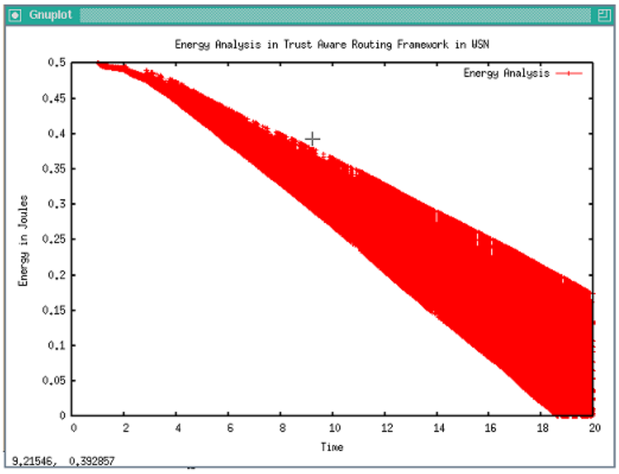

Fig 5.Energy Analysis of TARF

5 REFERENCES

[1].Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" vol.9, 2012.

[2]. S. Chang, S. Shieh, W. Lin, and C. Hsieh, "An efficient broadcast authentication scheme in wireless sensor networks," in Proceedings of the 2006 ACM Symposium on Information, computer and communications security (ASIACCS '06). New York, NY, USA: ACM, 2006, pp. 311–320.

[3].C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[4]. A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," Wireless Networks Journal (WINET), vol. 8, no. 5, pp. 521–534, Sep. 2002.

[5].A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proceedings of the 7th international conference on Information processing in sensor networks (IPSN '08). IEEE Computer Society, 2008, pp. 245–256.

[6]. R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04). New York, NY, USA: ACM, 2004, pp.59–64.

[7]. C. Karlof, N. Sastry, and D.Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in Proc. of ACM SenSys 2004, Nov. 2004.