IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Design of Trust Aware Routing Framework

Zeeshanali Shaikh[1], B.B. Gite[1]

Sinhgad Academy of Engineering, Pune[1]

Abstract: Wireless Sensor Networks (WSN) consist of Nodes, there can be several hundreds or even thousands. Node is built of several parts i.e. a radio Transceiver with an internal antenna, microcontroller, and an electronic circuit for interfacing. Nodes are controlled to specific base station which they are associated .WSNs can be applied in various fields i.e. Military Applications , Health Care Application, Forest Fire Detections, area monitoring etc. .Wireless Sensor Networks i.e. WSNs are exposed to various attacks such as Sinkhole attacks, Wormhole attacks, Sybil attacks .The major concern in WSNs is security ,only Cryptographic Techniques are not beneficial for solving severe problems .There are routing protocols such as Ambient Trust Sensor Routing (ATSR), Time Analysis Resilient Protocol (TARP), Feedback Based Secure Routing (FBSR) etc. which help in protecting WSNs from the attacks but some severe attacks cannot be addressed from the above routing protocols .Severe problems such as Identity deception through replaying routing information ,this may help in launching other attacks which were mentioned .TARF (Trust Aware Routing Framework) is effective against such attacks .TARF can be embedded with other routing protocols which exists and hence provided a secured network for data transmission.

Index Terms: WSN, TARF, ATSR, FBSR, TARP, Trust- Manager, Energy-Watcher.

1. INTRODUCTION

Wireless sensor networks (WSNs) applies mainly for military applications, Health care monitoring, forest fire monitoring. A WSN comprises battery-powered sensor nodes with extremely limited processing capabilities. WSN is network made up of a numerous small, low cost sensors nodes which collect and dis-seminate the data in particular situation. Sen-sor nodes communicate to the base station wirelessly by taking a multi-hop path. In a multi-hop path packets need to traverse from a multiple nodes before reach to the desti-nations which is a base stations. WSN tech-nology needs to use a cost effective path to transfer a packets from source to destinations. The physical security of a sensor node can be achieved by using a durable materials for designing a nodes which protect nodes from adversary physical attacks. The primary goals of WSN are to guarantee integrity, authenticity, availability of message in presence of a ad-versary in a communication system. However, the WSN multi-hop routing often prone to the different types of malicious attacks likewise selective forwarding attack, wormhole attacks, sinkhole attacks and Sybil attacks. An attacker may physically tamper nodes, attract or repel network traffic, partition network, create traffic collision with seemingly valid transmission, jam the communication channel It is also sus-ceptible to identity deception which are the main concern in the designing of the WSN.

2. LITERATURE SURVEY

2.1 Attacks on WSN

1) Sybil Attacks : In a Sybil attack, the WSN is subverted by a malicious node which forges a large number of fake identities in order to disrupt the networks protocols.It significantly affect on a fault tolerance and causes threat to the geographical routing protocol.

2) Wormhole Attacks: Wormhole nodes fake a route that is shorter than the original one within the network; this can confuse rout-ing mechanisms which rely on the knowledge about distance between nodes. It has one or more malicious nodes and a tunnel between them.

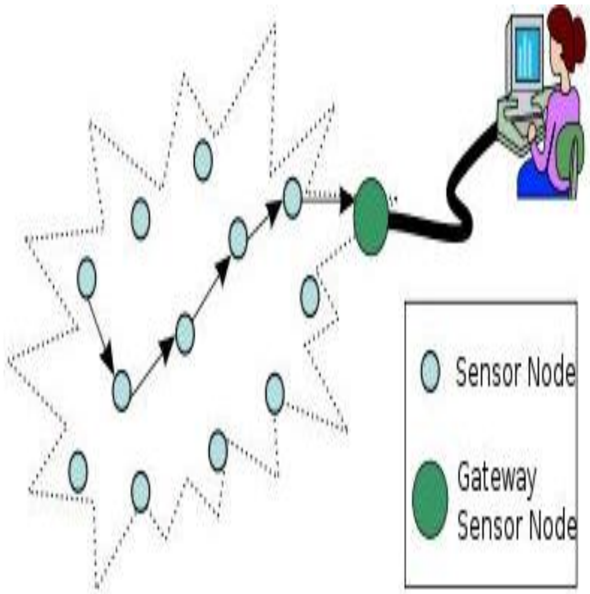


Fig1 Basic Multi-hop Routing In WSN

The attacking node captures the pack-ets from one location and transmits them to other distant located node which distributes them locally. A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mech-anisms.

3) Selective Forwarding: In a Selective for-warding adversary nodes can selectively drop only certain packets.

DOI 10.17148/IJARCCE.2016.5683

In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbours might start using another route. Now, with-out proper protection from all these attacks it is harmful to use WSN for routing packets. Thus to secure WSN, we have developed TARF (Trust aware routing framework). TARF is completely based on two components called as TRUST-MANAGER and ENERGY WATCHER. These components are necessary to analyse the trustworthiness and energy efficiency of each and every node that is going to take part in routing the packets through multihop path. TARF proves resilient under various attacks exploiting the replay of routing information. TARF is effective against identity deception.

4) Sinkhole Attack: In a Sinkhole attack an adversary nodes tries to attract traffic from a particular area to pass through a compromised nodes, thereby creating sinkhole with adver-sary at the center. In this attack, the goal of attacker is to attract nearly all the traffic from a particular area through a compromised node. This attack steals the valid identity of node. An adversary node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a black hole.

2.2 Security Issue In WSN

As the sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. The security goals are classified as primary and secondary [5]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, SelfOrganization, Time Syn-chronization and Secure Localization.

1) Data Confidentiality It is the ability to hide message from a passive attacker and is the most important issue in network security. Sen-sor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a WSN. Moreover, sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack.

2) Data Integrity and Authentication Integrity refers to the ability to confirm the message has not been tampered or altered while it was on the network. An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Indeed, data authentication allows a receiver to verify that the data really is sent by the claimed sender.

3) Data Availability Availability is of impor-tance for maintaining an operational network.
It is the ability of a node to utilize the resources and the network is available for the message to move on.

4)Scalability: The dynamic environmental condition, number of sensor nodes in a WSN, magnitude of the nodes, even the topology of the sensor network keeps changing very fre-quently to allow insertion of new fresh nodes and deletion of fused nodes in a network . However, an extension or reduction of the sen-sor network or replacement of any unreliable physical objects should not affect the perfor-mance of the WSN. That is why scalability in the security solution is mandatory.

2.3 Existing Routing Protocols and Demer-its

It is generally hard to protect WSNs from wormhole attacks, sinkhole attacks and Sybil attacks based on identity deception. There are certain protocols that secure WSN but are not sufficient to protect it totally, these protocol are FBSR [5], ATSR [4], and TARP [6].

1) Ambient Trust Sensor Routing (ATSR): The ATSR protocol is a location based trust aware routing solution. ATSR incorporated dis-tributed trust model which relies on both direct and indirect trust information to protect WSN from a wide set of routing and trust related attack. ATSR follow the geographical approach which is inherently immune against a set of attack. Both direct and indirect trust informa-tion is taken into account to evaluate the trust-worthiness of each neighbour. An important feature of the proposed routing solution is that it takes into account the remaining energy of each neighbour, thus allowing for better load balancing. ATSR bases the next hop neighbour selection not only on location coordinates but also on energy and trust based on a routing cost function. ATSR protect the WSNs from packet missforwarding, packet manipulation and ac-knowledgements spoofing. ATSR fails to offer protection against the identity deception like as FBSR through replaying routing information.

2) Time Analysis Resilient Protocol (TARP): TARP is in practice to protect the WSN from the timing analysis attacker whose intention is to know the information about WSN user nodes,

3) Application running on nodes, and study of a network by performing analysis on a trans-mission pattern of a network. The attacker can find out this information even when the traffic is encrypted. TARP is a traffic mixing approach for defeating timing analysis which is performed towards sensor networks. TARP, defeats the timing analysis attack by forming a single frame of a multiple packets which are destined for the different node of a network. In TARP all nodes transmit using identical pat-terns, completely decorrelating transmissions from data, and making all nodes appear identi-cal. TARP does not offer protection against the identity deception through replaying routing information.

4) Feedback Based Secure Routing (FBSR): In FBSR protocol each node which is a part of a WSN gathered the feedback from its neighbor-ing nodes before forwarding the packets to the base station. The FBSR gives the

DOI 10.17148/IJARCCE.2016.5683

dynamic infor-mation about the WSN to each of its nodes. The feedback message is to be used to gather an information about a WSN network this feedback message present in a acknowledgment frame of a MAC layer. The authentication of a each feedback message can be done by using keyed one way hash Chain (Keyed-OWHC) to avoid feedback fabrication. FBSR takes a independent forwarding decision based on a feedback of a network and also predict a future circumstance on the basis of this feedback gathered infor-mation. The FBSR fails to offer a protection against wormhole attack. The authentication system which is to be used in FBSR by using Keyed-OWHC- causes considerable overhead in a communication.

3. PROBLEM DEFINITION SCOPE OF PROPOSED SYSTEM

3.1 Goals and Objectives

TARF mainly guards a WSN against the attacks misdirecting the multi-hop routing, especially those based on identity theft through replaying the routing information. TARF aims to achieve the following desirable properties:

1) High Throughput: Throughput is defined as the ratio of the number of all data packets delivered to the base station to the number of all sampled data packets. In our evaluation, throughput at a moment is computed over the period from the beginning time (0) until that particular moment. Note that single-hop re-transmission may happen, and that duplicate packets are considered as one packet as far as throughput is concerned. Through- put reflects how efficiently the network is collecting and delivering data. Here we regard high through-put as one of our most important goals.

2) Energy Efficiency: Data transmission ac-counts for a major portion of the energy con-sumption. We evaluate energy efficiency by the average energy cost to successfully deliver a unit-sized data packet from a source node to the base station. Note that link-level re-transmission should be given enough attention when considering energy cost since each re-transmission causes a noticeable increase in energy consumption. If every node in a WSN consumes approximately the same energy to transmit a unit-sized data packet, we can use another metric hop-per-delivery to evaluate energy efficiency. Under that assumption, the energy consumption depends on the number of hops, i.e. the number of one-hop transmissions occurring. To evaluate how efficiently energy is used, we can measure the average hops that each delivery of a data packet takes, abbrevi-ated as hop-per-delivery.

3) Scalability Adaptability: TARF should work well with WSNs of large magnitude un-der highly dynamic contexts. We will evalu-ate the scalability and adaptability of TARF through experiments with large-scale WSNs and under mobile and hash network condi-tions.

3.2 Design of TARF

TARF is energy efficient, highly scalable, and well adaptable. TARF has two components trust manager [1] and energy watcher [1] for calculating the trustworthiness and energy cost of each node of a WSN. Every nodes of a WSN have its neighbourhood table which gathered the valve of energy cost and trustworthiness of a next node in a network, which is computed by trust-manager and energy-watcher. TARF secures the multi-hop routing in WSNs against intruders by evaluating the trustworthiness of neighbouring nodes. It identifies such intruders by their low trustworthiness. It also checks for energy for next node. If energy required for routing of packet is less than it routs data to that node. But this job is strictly done after checking the trustworthiness of next node. In TARF, in addition to data packet transmission, there are two types of routing information that need to be exchanged: I) Broadcast messages from the base station about data delivery. II) Energy cost report messages from each node.
A broadcast message from the base station is given to each and every node in routing path throughout the whole network. Energy Watcher is responsible for recording the en-ergy cost for each known neighbour, one hop transmission to reach its neighbours and the energy cost report from those neighbours. A compromised node may falsely report an ex-tremely low energy cost to attract its neigh-bours into selecting this compromised node as their next hop node. However, these TARF enabled sensor neighbours nodes eventually cease to select that compromised next hop node based on its low trustworthiness as tracked by Trust Manager. Trust Manager is responsible for tracking trust level values of neighbours based on network loop discovery and broad-cast messages from the base station about data delivery.

WORKING OF EACH NODE: In above fig 2, we can see that each node has its own neighbourhood table. Now Node A, when it wants to send packet to next node then ener-gywatcher and trust-manager of node A check the energy cost and trustworthiness of next node. The node which is efficient is selected for next hop In multi-hop environment. The value of energy cost and trustworthiness of that node is stored in neighbourhood table of node A. And once next node is decided for its next hop neighbourhood table [1] sends out its energy report message it broadcasts to all its neighbours its energy cost to deliver a packet from the node to the base station. The neighbourhood table manages all the records of routing of each node In a WSN.

ANALYSIS OF ENERGY WATCHER AND TRUST MANAGER: For this, let us consider an example node A, B, C and D are all legitimate nodes and not compromised. Node A has node B as its current next-hop node while node B has an attacker node as its next hop node. The attacker drops every packet received and thus any data packet passing node A will not arrive at the base station. After a while, node A discovers that the data packets it forwarded did not get delivered.

DOI 10.17148/IJARCCE.2016.5683

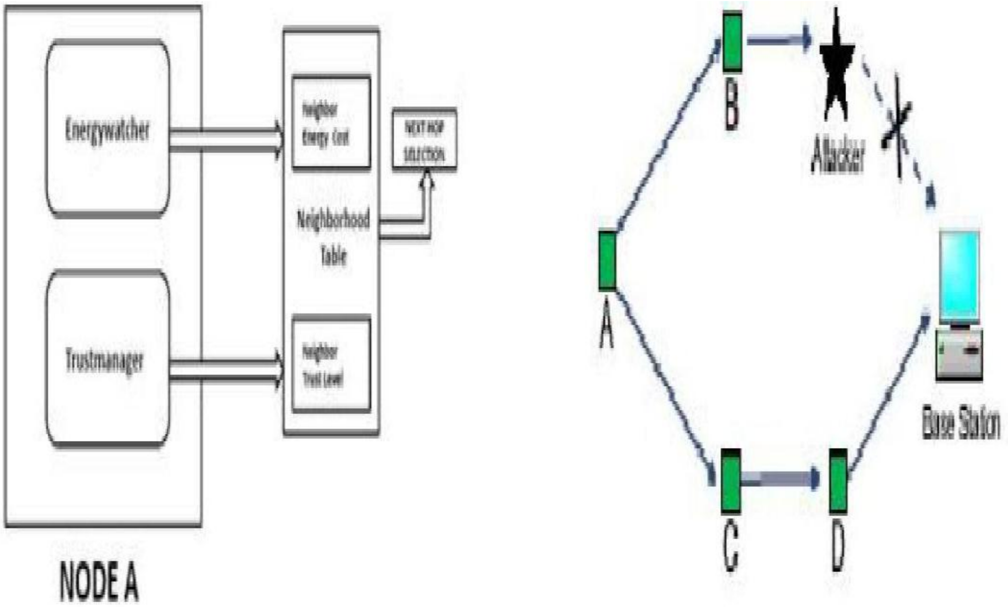


Fig.2 Block Diagram of Each Node In TARF

The Trust Manager on node A starts to degrade the trust level of its current next-hop node B although node B is absolutely honest. Once that trust level becomes too low, node A decides to select node C as its new next-hop node. In this way node A identifies a better and successful route (A - C - Dbase). In spite of the sacrifice of node Bs trust level, the network performs better. Further, concerning the stability of routing path, once a valid node identifies a trustworthy honest neighbour as its next hop node, it tends to keep that next hop selection without considering other seemingly attractive nodes such as a fake base station.

3.3 DESIGN CONSIDERATIONS

TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TARF is also energy- efficient, highly scalable, and well adaptable. Before introducing the detailed de-sign, we first introduce several necessary no-tion here. Neighbor For a node N , a neighbor (neighboring node) of N is a node that is reachable from N with one-hop wireless trans-mission. Trust level For a node N , the trust level of a neighbor is a decimal number in [0, 1], representing N s opinion of that neighbors level of trustworthiness. Specifically, the trust level of the neighbor is N s estimation of the probability that this neighbor correctly delivers data received to the base station. That trust level is denoted as T in this paper. Energy cost For a node N , the energy cost of a neighbor is the average energy cost to successfully deliver a unit-sized data packet with this neighbor as its next-hop node, from N to the base station. That energy cost is denoted as E in this paper.

Overview : For a TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighbouring node it should forward the data packet considering both the trustworthiness and the energy efficiency. Once the data packet is forwarded to that next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors.It is sometimes necessary to delete some neighbors entries to keep the ta-ble size acceptable. The technique of maintain-ing a neighborhood table of a moderate size is employed by TARF. A broadcast message from the base station is flooded to the whole network. In TARF, in addition to data packet transmission, there are two types of routing information that need to be exchanged: broad-cast messages from the base station about data delivery and energy cost report messages from each node. Neither message needs acknowl-edgement. A broadcast message from the base station is flooded .The freshness of a broadcast message is checked through its field of source sequence number. The other type of exchanged routing information is the energy cost report message from each node. For each node N in a WSN, to maintain such a neighbourhood table with trust level values and energy cost values for certain known neighbors, two components, EnergyWatcher and TrustManager, run on the node (Figure 2).

EnergyWatcher is responsible for recording the energy cost for each known neighbor, based on N s observation of one-hop transmission to reach its neighbors and the en-ergy cost report from those neighbors. A com-promised node may falsely report an extremely low energy cost to lure its neighbors into select-ing this compromised node as their next-hop node; however, these TARF-enabled neighbors eventually abandon that compromised next-hop node based on its low trustworthiness as tracked by TrustManager. TrustManager is responsible for tracking trust level values of neighbors based on network loop

DOI 10.17148/IJARCCE.2016.5683

discovery and broadcast messages from the base station about data delivery. Once N is able to decide its next-hop neighbor according to its neigh-borhood table, it sends out its energy report message: it broadcasts to all its neighbors its energy cost to deliver a packet from the node to the base station. The energy cost is computed as in Section 3.3 by EnergyWatcher. Such an energy cost report also serves as the input of its receivers.

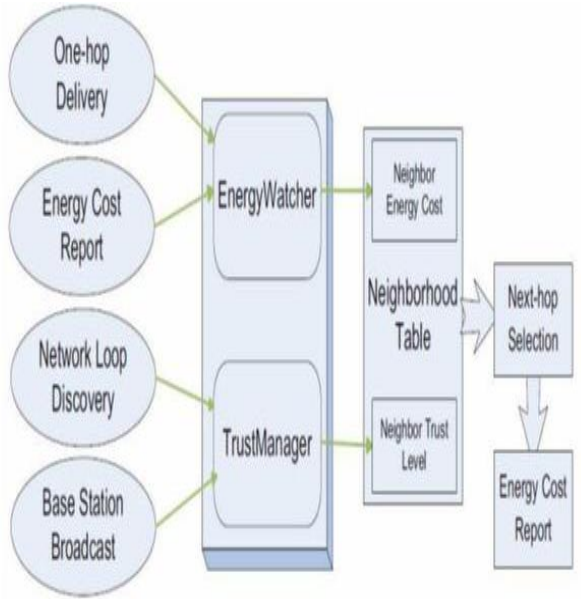


Fig. 4. WSN Modules

Fig. 4. Each node selects a next-hop node based on its neighborhood table, and broad-cast its energy cost within its neighborhood. To maintain this neighborhood table, Energy-Watcher and TrustManager on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbors.

4. IMPLEMENTATION DETAILS

A) Design:
For a node N, a neighbour (neighbouring node) of N is a node that is reachable from N with one-hop wireless transmission. Trust level for a node N, the trust level of a neighbour is a decimal number in [0, 1], representing Ns opin-ion of that neighbours level of trustworthiness. Specifically, the trust level of the neighbour is Ns estimation of the probability that this neighbour correctly delivers data received to the base station. That trust level is denoted as T. Energy cost For a node N, the energy cost of a neighbour is the average energy cost to suc-cessfully deliver a unit-sized data packet with this neighbour as its next-hop node, from N to the base station. That energy cost is denoted as E. For a TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighbouring node it should forward the data packet considering both the trustworthiness and the energy efficiency. Once the data packet is forwarded to that next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. N maintains a neigh-bourhood table with trust level values and en-ergy cost values for certain known neighbours by energy-watcher and trust manager. There are additionally two information apart from routing which are broadcast message from base station about data delivery and energy cost report from each node. A broadcast message from the base station consists node id of a source node, an undelivered sequence interval [a, b] with a significant length. Accordingly, each node in the network stores a table of node id of a source node, a forwarded sequence interval [a, b] with a significant length.

B) Input:
Select Draw no of nodes. Select Source and Destination.

C) Output:
Finds the neighbour for according to energy level and trustworthiness.
Malicious nodes will be excluded and the node who has threshold energy level and trust-worthiness will be selected for communication.

4.1 Algorithmic Details

Algorithm to detect trustworthiness of node N:

A) For a node N to select a route for delivering data to the base station.
B) N will select an optimal next-hop node from its neighbours based on trust level and energy cost and forwards the data to the chosen next hop node immediately.
C) The neighbours with trust levels below a certain threshold will be excluded from being considered as candidates.
D) Among the remaining known neighbours, N will select its next-hop node through evalu-ating each neighbour b based on a trade- off between TNb and (ENb/TNb), with ENb and TNb being bs energy cost and trust level value in the neighbourhood table a node Ns.

Algorithm to check energy cost of node N:

A) Energy Watcher computes the energy cost ENb for its neighbour b in Ns neighbourhood table and N decides its own energy cost EN.
B) Here, ENb mentioned is the average en-ergy cost of successfully delivering a unit sized data packet from N to the base station, with b as Ns next hop node being responsible for the remaining route.
+ Here, one hop retransmission may occur until the acknowledgement is received or the number of retransmissions reaches a certain threshold. The cost caused by one-hop retrans-missions should be included when computing ENb.Suppose N decides that A should be its nexthop node after comparing energy cost and trust level. Then Ns energy cost is EN = EN Denote EN-b as the average energy cost of successfully delivering a data packet from N to its neighbour b with one hop. Note that the retransmission cost needs to be considered. With the above notations, straight forward way to establish the following relation: ENb = ENb + Eb.

DOI 10.17148/IJARCCE.2016.5683

4.2 Mathematical Evaluation

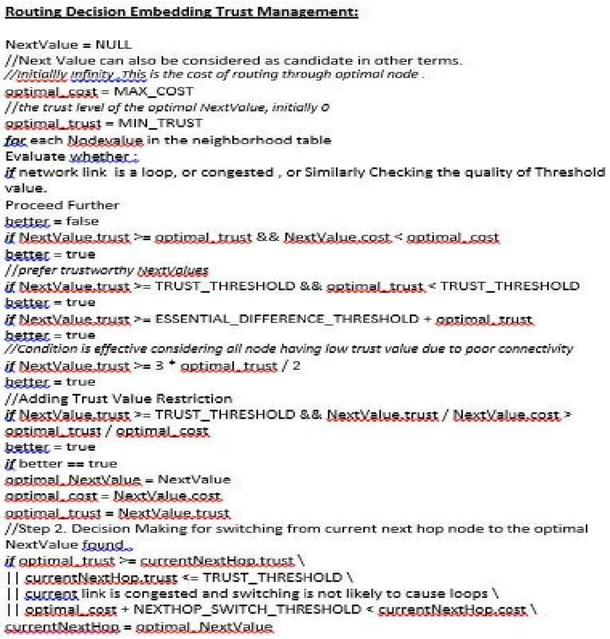
Calculation of Trust Value: $Tnew_N$ b = (1 w):$Told_N$ b + w:d

Where $Told_N$ bisCalculatedtrustvalue(Last); w is the weight assigned to the delivery ratio in the last observation window d (Delivery ratio) is the ratio of successfully delivered to the sink packets over the transmit-ted packets.

Calculation of Energy Watcher: ENb = Eunit/Psucc + Eb

Where ENb is energy cost of node N trans-mitting a packet to the sink node (attacked node) through the path passing from neigh-bor b and Psucc is the probability of a ac-knowledged transmission, the retransmissions are considered.

4.3 Algorithm for Decision Making on the basis of Neighbourhood table values



```
Routing Decision Embedding Trust Management:

NextValue = NULL
//Next Value can also be considered as candidate in other terms.
//initiallly infinity .This is the cost of routing through optimal node .
optimal_cost = MAX_COST
//the trust level of the optimal NextValue, initially 0
optimal_trust = MIN_TRUST
for each Nodevalue in the neighborhood table
Evaluate whether :
if network link  is a loop, or congested , or Similarly Checking the quality of Threshold
value.
Proceed Further
better = false
if NextValue.trust >= optimal_trust && NextValue.cost < optimal_cost
better = true
//prefer trustworthy NextValues
if NextValue.trust >= TRUST_THRESHOLD && optimal_trust < TRUST_THRESHOLD
better = true
if NextValue.trust >= ESSENTIAL_DIFFERENCE_THRESHOLD + optimal_trust
better = true
//Condition is effective considering all node having low trust value due to poor connectivity
if NextValue.trust >= 3 * optimal_trust / 2
better = true
//Adding Trust Value Restriction
if NextValue.trust >= TRUST_THRESHOLD && NextValue.trust / NextValue.cost >
optimal_trust / optimal_cost
better = true
if better == true
optimal_NextValue = NextValue
optimal_cost = NextValue.cost
optimal_trust = NextValue.trust
//Step 2. Decision Making for switching from current next hop node to the optimal
NextValue found..
if optimal_trust >= currentNextHop.trust \
 || currentNextHop.trust <= TRUST_THRESHOLD \
 || current link is congested and switching is not likely to cause loops \
 || optimal_cost + NEXTHOP_SWITCH_THRESHOLD < currentNextHop.cost \
currentNextHop = optimal_NextValue
```

Fig. 5. Algorithm for Routing

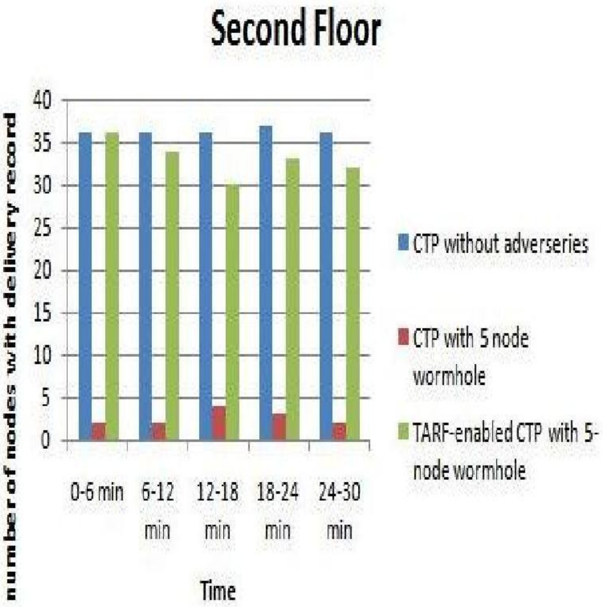


Fig. 7. First Level

5. EMPIRICAL EVALUATION

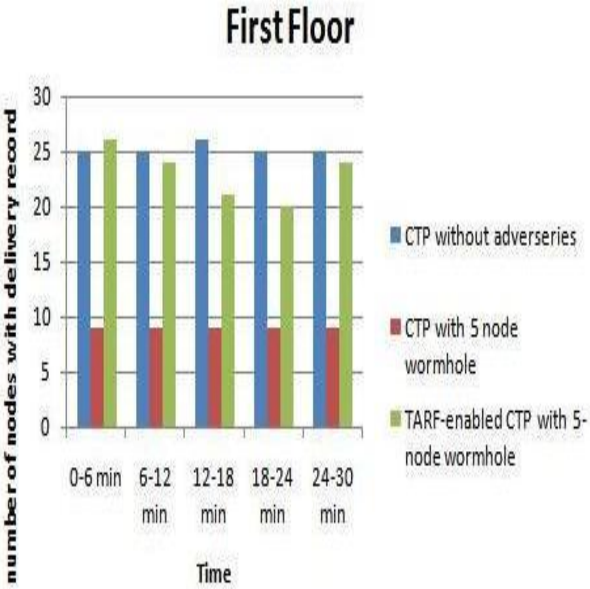


Fig. 6. Energy Comparison Chart

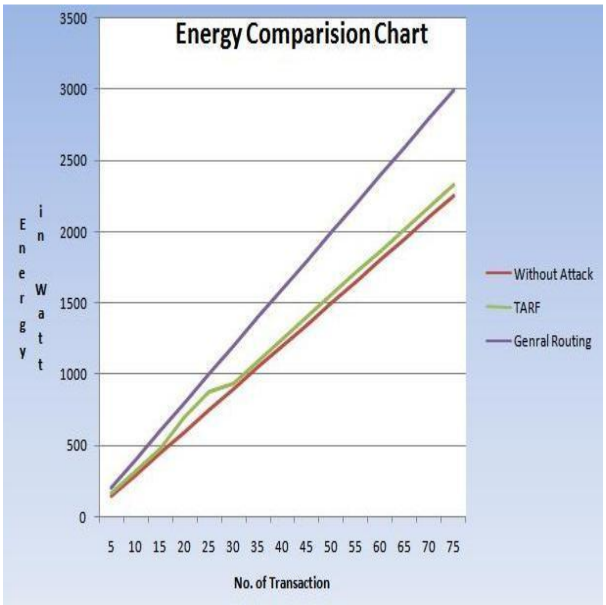


Fig. 8. Second Level

DOI 10.17148/IJARCCE.2016.5683

6. CONCLUSION

We have tried to focus on implementation of improved Trust Aware Routing System which enhance security to dynamic WSNs. TARF pro-vides trustworthiness and energy efficiency which are important for the survival of a WSN in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. We have de-signed and implemented TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of rout-ing informationt. TARF focuses on trustwor-thiness and energy efficiency, which are vital to the survival of a WSN in a hostile envi-ronment. With the idea of trust management, TARF enables a node to keep track of the trust-worthiness of its neighbors and thus to select a reliable route. Our main contributions are listed as follows. (1) Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information. (2) The resilience and scalability of TARF is proved through both extensive simula-tion and empirical evaluation with large-scale WSNs; the evaluation involves both static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks. (3) We have implemented a ready-to-use TinyOS module of TARF with low overhead; as demonstrated in the paper, this TARF module can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully-functional protocols. (4) Finally, we demonstrate a proof-of-concept mobile target detection application that is built on top of TARF and is resilient in the presence of an anti-detection mechanism; that indicates the potential of TARF in WSN applications.

REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, Tarf: A trust-aware routing framework for wireless sensor networks, in Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN10), 2010.

[2] F. Zhao and L. Guibas, Wireless Sensor Networks: An In-formation Processing Approach. Morgan Kaufmann Pub-lishers, 2004.

[3] [A. Wood and J. Stankovic, Denial of service in sensor networks, Computer, vol. 35, no. 10, pp. 5462, Oct 2002.

[4] 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.

[5] M. Jain and H. Kandwal, A survey on complex wormhole attack in wireless ad hoc networks, in Proceedings of International Con-ference on Advances in Computing, Control, and Telecommunication Technologies (ACT 09), 28-29 2009, pp. 555 558.

[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, Launching a sink- hole attack in wireless sensor networks; the intruder side, in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Com-munications(WIMOB 08), 12-14 2008, pp. 526 531.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, The sybil attack in sensor networks: Analysis and defenses, in Proc. of the 3rd International Conference on Information Processing in Sensor Networks (IPSN04), Apr. 2004.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, Performance analy-sis of mobile agent-based wireless sensor network, in Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009), 20-24 2009, pp. 16 19

DOI 10.17148/IJARCCE.2016.5683