International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-5, March 2019

Trustworthy Routing in Wireless Sensor Networks Using Hop Count Filter

Pritesh A. Patil, R. S. Deshpande

Abstract: ***Wireless Sensor Networks transmit data from source to destination and inform base station using various sensors. However, the routing path through multiple hops of WSNs usually becomes the target of severe attacks. Outmoded cryptographic security techniques have proven to be inefficient against several insider attacks such as wormhole attack, sinkhole attack, Sybil attack, selective forwarding attack, etc. These attacks further impacts on restating of routing information and also exacerbate identity deception. To handle such instances, trust aware routing can be the alternative to provide a trustworthiness and energy efficient route irrespective of known geographic information or tight time synchronization. Significantly, it is strong against the attacks caused due to identity theft. Besides that WSNs are also vulnerable to the attacks illegally acquiring network resources which is caused by many popular attacks. These attacks are complex as it affect not only the victim but its legitimate members also. Existing routing techniques could not solve these severe issues. We are proposing an effective solution, M-TARF to significantly defend network from annoying resource acquisition imposed by adversaries on compromised nodes and its neighbours through additional component hop_count_filter. The proposed scheme demonstrated an average throughput of 6.4% which is more that existing scheme when implemented on NS2 for varying number of nodes.***

Index Terms**: *Hop count filter, Supervisor, Trust_advisor, Energy_recorder, hop_count.***

I. INTRODUCTION

Networks of wireless sensor nodes are revolution in mobile computing with cost effectiveness, lower maintenance at field locations. This network usually have several lower-cost and power and versatile sensors which are dispersed all over the field of requirement. The sensor nodes are very small in size but are loaded with sensing capabilities, microprocessor, transceivers and internal memory. They wirelessly interact with each other over limited range as well as help each other to perform the assigned task to the network viz wild animal tracking in forest region.

Now a days, WSN positioned on a variety of applications which includes security of private land, army and hospitals. Nodes of the sensor network installed and functioned in these kind of places are targets of many attacks viz. black, sink and worm hole, diversion of path, duplication and hello flooding attacks. Hence development routing protocol for sensor networks with security and energy efficiency to secure them from these attacks alongside effective utilization of the energy of nodes is essential. For WSNs many of the routing schemes have been proposed. Majority of them considers rigid nodes and base station for gathering data from fields on which the network is formed. Nevertheless, the objects on which the sensor nodes are mounted may be moving in nature and latest improvements indicates movable sensors nodes in WSNs fulfils the requirement of expected performance. This paper surveys various proposed routing schemes for WSNs and shows the security problems related with the existing routing schemes alongside discuss a secure trust aware routing framework providing secured transmission of packets resistant to most of the attacks. The implementation details with the screen shots of the system have been shown in sixth section.

WSNs are deployed in numerous fields such as private lands, hospitals, nature monitoring and army applications for the collection of on field data frequently which may be complex or rather difficult and costly with wired network of sensors. On these factors several applications are proposed which includes animal behaviour, environmental and craft including aeroplane, vehicle as well as ships monitoring[3]. Networks may consist of many sensor nodes may be upto thousands in number which are of less power, economical nodes, probably non static however mostly fixed at predefined position, installed to observe the effect of environment. Central control called base station is there in almost all sensor networks. It usually act as bridge between the networks, also its data processing capabilities are high which makes it act as data centre or interface for users. The use of base station can be as a nexus for disseminating control information among the nodes of network or extract data from them. Continuous data set such as every second the reading of sensor from the nodes satisfying the query, may be requested by base station. The stream of data is referred to as data flow and the node originating it as source. To control the energy, all sensor readings are combined and then processed through the point of aggregation. This forwarded single message contains the reading obtained from various nodes which is the aggregated value. Due to simplicity of many routing schemes they become vulnerable to attacks such as wormhole, sink hole Sybil and denial of service. The malicious node caused by wormhole attack, forges the identity of the legitimate node and use that wrong identity to participate in the false routing in, which will be troublesome for actual traffic of network[17]. Sinkhole attack caused wrong route replies by adversary to requested routes it receives, alongside publicising itself as having shortest route to the destination.

These wrong route replies tends to divert the traffic through malicious node for snooping. [1].

Manuscript published on 30 March 2019.
***Correspondence Author(s)**
Pritesh A. Patil, E&TC Department, VIIT Pune, Affiliated to Savitribai Phule Pune University, Maharashtra, India
Dr. R. S. Deshpande, Principal, SCSMCOE, Nepti, Ahmednagar, Affiliated to Savitribai Phule Pune University, Maharashtra, India

In Sybil attack, the malicious node projects multiple identities in network also repeating the routing information. [3] The accidental failure of nodes or any malevolent act causes Denial of Service (DoS). DoS not only try to overthrow, interrupt, or abolish the network, but also resist the network to perform or participate in routing service. DoS can be realized in various layers of sensor networks.[2]

This attempt is making these networks susceptible to severe threats and attacks.

Hence it became essential to integrate security techniques to secure crucial data flow over the network. The already proposed systems are nonviable as they incurs overheads and more cost. Our main focus is to strengthen the network by confronting several severe attacks alongside limiting the overheads and realize better approximation in case of throughput. Moreover our target is to implement security in proposed routing system in the network.

Following is the organization of the rest of the paper: Related work is described in section 2. Section 3 deals with the concerns in design of the proposed system. Design of the proposed trustworthy routing is elaborated in Section 4. Section 5 gives the analysis of energy_recorder and trust_advisor. Performance evaluation of the proposed system is presented in section 6. Finally section 7 concludes the paper.

II. RELATED WORK

Decency, energy efficacy and trial to bypass the illegal involvement of nodes by encoding the data and verifying the packets are the main focus in existing routing schemes developed for WSNs. Some of the encoding and verification schemes are discussed in[13]. Li [5] proposed TAODV protocol in which the trust relationship between the nodes is calculated to detect malicious nodes. Its security mechanism is based on public key encryption which causes extra computational overhead. In TAODV key management is self-organized to maintain the trusted relation among the nodes. This asymmetric key calculation and trust relation building would be the major constraints for WSNs because of which TAODV is not suitable for Sensor networks. Gong et al [6] presented the TRANS protocol to develop faithfulness among the source and sink nodes. Unauthorized node entry is restricted in the network by using asymmetric verification for trusted routing. It is considered that the self as well as neighbouring node's locations are known to the sensors by geographic routing and to authenticate the message reaching base station is done by shared encoding to realize privacy. The base station replies only through the valid and trusted neighbours. Ambient trust sensor routing (ATSR) designed in [7], which incorporates a distributed trust model (DTM). DTM's functioning depends on direct trust information (DTI) and indirect trust information (ITI) to defend WSN against attacks. In ATSR, nodes calculate DTI per neighbour by observing the behaviour of their neighbouring node based on trust value. ITI is obtained by the nodes by requesting it from the neighbour of neighbours to rapidly enhance the trust chain. ITI is also termed as reputation. Total trust information (TTI) is obtained by adding DTI and ITI. At the end, based on the distance to the base station i.e. geographic position information and TTI the routing decision is taken. However frequent advertisement of the position of nodes, energy level and reputation request for getting ITI involve significant overhead and makes ATSR vulnerable to ientity deception attacks.

Three security concerns discussed in the ad-hoc networks in [8], firstly, the use of wireless link is highly susceptible to link attacks passively and actively, secondly, due to lack of physical protection to nodes, they can easily be captured and compromised, and due to dynamic change in the network any security solution with fixed configuration will not be enough. Fair and rational security mechanism is been introduced into Ad-Hoc networks. Trust is defined in this technique as the confidence of personal trusted bubble (PTB) on the other PTB built on the faith and expectations that action is very important. The trust matrix is used to store the knowledge for trust evaluation on other bubbles. Due to the operations and complex calculations this strategy incurs considerable overhead. Also it targets only the powerful devices hence not suitable for the limited computation capability and powered WSNs. TARP for Sensor ctuator Networks only keeps track of node's routing strategy and quality of the link to determine effective path from nodes to base station[9]. TARP lets the routing messages to be sent by nodes to the base station. Cooperation by their neighbours is termed as trust which is the likelihood that it forwards its neighbour's messages. TARP keeps track of cooperation as reputation. TARP's routing process is divided in two concurrent phases first is Reputation Assessment and the other is Path Reliability Evaluation. TARP only works based on the reputation that the nodes have with others. This will lead to the case where due to false identity broadcasted, malicious nodes and adversaries will get an opportunity to get through the network. Also TARP incurs considerable overhead during routing. The TRIDNT in ad-hoc network to deal with misbehaviour proposed by Ali et al [10]. In this the nodes are declared themselves as their neighbour. This self trust was measured in termed as selfishness degree which is used to reduce the searching time of misbehaving node. TRIDNT used data link layer-acknowledgement (DLL-ACK) and TCP-ACK to monitor the degree of selfishness based on those nodes' trust values that are direct and indirect. But TRIDNT is not capable to handle more than one malicious node also degree of selfishness is not promising against identity theft. Whereas in FBSR, based on the feedback from neighbours nodes decide whether to forward the data packet along with security and energy efficiency or not. Congestion in the network is avoided by including this feedback in the ACK frame. Feedback manipulation is restricted through keyed one way hash chain. Feedbacks of both neighbours and base station are taken in to account to determine the trust. But the technique used in FBSR for authentication incurs considerable overhead. Defence against identity theft is not been tested and evaluated [11].CBTRP developed [12] for mobile networks to protect them against selective forwarding attack. CBTRP arranges the clusters and kept them at one-hop distance then will elect the cluster head based of the current specifications of the node. Responsibility of handling all activities of routing in the network is of the cluster heads. Cluster heads are frequently replaced when they become infected and update the packet forwarding path at run time or dynamically. But it focuses only on the powerful nodes of the network which causes the other underestimated nodes to become target of the identity theft related attacks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Also CBTRP incurs excessive computational overhead in terms of cluster formation, cluster head selection, checking the health of cluster head, replacing it, routing process. Because of these constraints CBTRP is not suitable for WSNs.

Another strong implementation is TARF for WSNs to make secure routing involving multiple hops against severe attacks. The main focus of the design is trustworthiness and energy efficiency which are crucial factors for the survival of WSNs in Harsh environmental conditions. Trustworthiness of the neighbouring nodes is been tracked by the node to select a reliable path. It does not demand any tight time organization and the geographic location of the node. TARF can only defend the WSN against Sinkhole and Sybil identity deception attacks using replaying routing information [13] and does not provide protection against the DoS also if the links are weaker then there is no provision for alternative routing path as a result the communication will be simply terminated.

In TSRF the trust is calculated for both nodes as well as link of the routing path. For node the direct and indirect trust values are evaluated [14]. Evaluation of direct trust involves the neighbouring node's past behaviour is taken into account in this scheme. Whereas the indirect trust is evaluated based on the trust chain as stated in [7]. However frequent advertisement of the position of nodes, energy level and reputation request for getting trust chain based indirect trust values incurs considerable computation overhead and energy overhead. Also exposing the network to adversaries stealing identity of nodes and path hijackers causing selective forwarding and act as balckhole.

Routing misbehaviour prevention scheme for wireless network by injecting dummy packet is proposed in [15]. In this dummy packet is inserted in obtained route to observe the packet dropping which helped the system to identify the node's misbehaviour in routing. Due to the use of fuzzy based trust model, this scheme incurs significant amount of overhead. Also it is vulnerable to many severe attacks caused by powerful nodes.

By considering energy as a crucial factor along with security Chen [16] presented, ETARP for WSN for minimizing energy consumption along with trustworthiness during the communication. In the packet format only hop count is replaced by energy cost and is used to estimate the energy cost in normal case when the network is attack free and separately when it is attacked. Trustworthiness of routes is calculated based on the expected utility of a specific route which is related to energy cost and trust level. ETARP estimates the risk in the network by using Bayesian network theory. This network is used to identify the nodes' status whether they are compromised or not. However the computational overhead is not exceptional in case of ETARP also along with identity and resource consumer attacks. Energy efficiency in ETARP is only effective in Normal case only as calculating the same in the presence of attacks makes the situation more complex.

TERP [18], a trust and energy aware routing scheme is proposed which isolates the misbehaving nodes through distributed trust model. Routing decisions are made based on the trust, energy and hop count of neighbour which are combined in the routing function. Unwanted route discovery is avoided in this method by pre-evaluation of the link termination.

Another attempt for improving the level of trust among nodes is made by Subbiah et. al. [19]. Alongwith direct and indirect trust, reachability of trusted node is determined by SSI. Trusted routing is assigned to neighbours on the successful match of sequence ID through logs. However scheme may become unstable if false route replies are made by compromised nodes.

At the outset, to secure WSNs routing strategies against these attacks causing damage to routing information we have designed a reliable, trust and energy efficient routing mechanism M-TARF by adding hop_count_filter in the existing design of [13]. The main focus of design is on three parameters now i.e. hop_count, trust and energy values which each node of the network calculate and maintain about their neighbours. However design of M-TARF mechanism may be autonomous and comprehensive but our determination is agreeing upon incorporation of our design with ease and hence making it reliable and complete solution. Nodes location information and time synchronization are not the requirements of our routing scheme unlike previous proposals. Reliable and with low control overhead network performance is observed even if the network is injected with severe attacks. The performance of our trust based routing scheme is confirmed through calculations and simulation. The simulation results show its effectiveness in terms of packet delivery ratio, throughput, energy efficiency and control overhead in both the cases of presence and absence of attacks.

III. CONCERNS IN DESIGN

Prior to the discussion on design of M-TARF, initially we would like to highlight some concerns in design including few conventions and then objectives.

3.1 CONVENTIONS

Data collection tasks belong to the most basic functions of WSNs. Securing these data collections under routing procedure is our main target. Transmission of tested data from node to base station with the help of in-between nodes is nothing but the data collection task shown in fig. 1. However there may be more than one base station but our scheme is unaffected by the presence of multiple base stations. For the simplicity we assume that there is only one base station. Next assumption is identity of legitimate node may be forged by the attacker by replaying routing information and misdirecting the acknowledgement packet; wormhole may do it remotely.

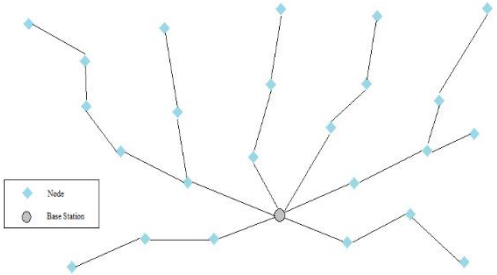


Figure 1. Multihop routing for data collection.

Data aggregation is out of our assumption for more simplification to introduce mechanism of M-TARF. However our scheme can still be applied to

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

WSNs in which data aggregation is carried at heads and then relayed such as cluster based approaches in WSNs. Aggregation of data from client nodes leads to energy efficiency and bandwidth. In clustered WSNs the heads from the sub-network and through this network only the data is routed to base station. Then our scheme can be applied to these sub-networks to realize secure routing. This framework may be executed on header node which communicate with its member nodes directly as fixed cluster has known relationship between a head and its member node and further security
at link may be incorporated. At the end data packet, fig. 2, is assumed to have following fields: sender id, sender sequence number, next-hop node id which is responsible for further processing of data packet to base station, source id this node initiates the data packet, source sequence number and hop_cnt value.

S_id	SSN	NN_id	Src_id	Src_SSN	H_cnt

Figure 2 Format of the data packet.

It is our recommendation of inclusion of source node's information for tracking the delivery of packet to base station. There would be enough control overhead while transmitting overall one_hop information to base station. Sequencing of routing packets is also of one of our assumption.

3.2 NEED OF AUTHENTICATION

Packets including broadcast packets from base station are required to be properly authenticated. In our approach asymmetric authentication is applied on broadcasting from base station to ensure inability of attackers to modify, change or forge the message. In M-TARF, before sending the broadcast message to trust_advisor even in presence of adversaries, we apply hop_count_filter to discard spoofed packets and pass on legitimate one. And then the trustworthy route is discovered based on delivery information by bypassing the affected nodes. Usually it is very difficult for the attacker to affect asymmetrically authenticate broadcast packet from base station. Thus authentication is crucial to realize secure routing.

Due to complexity in computation by asymmetric scheme and difficult management of key, normal packet may only be loosely symmetrically authenticated with limited set of keys as in TinySec[4] except broadcast from base station. But it will be possible for attacker to steal the identity of legal member node of the network and approved attempt of joining the network. Inspite of reception of traffic and after getting delivery information through broadcast packets, the legal member node of network which directly or indirectly responsible for forwarding that packet, will choose more reliable and trusted route using energy_recorder and trust_advisor.

3.3 OBECTIVES

The main aim of M-TARF is to protect WSN from the threat creating disturbance in the multihop routing procedure, precisely based on the deception of identity by replaying the routing information. For this we are addressing the attack which is causing network resource consumption and damage to network[3] through hop_count_filter. In this as stated earlier the nodes along with trust and energy values, maintains hop count values also. Matching of hop count present in packet, fig. 3, with the hop count publicised by node allowing to forward the packet to energy_recorder and then to trust_advisor for selecting the next potential neighour and checking the trustworthiness of same. Following are the desirable properties to which our M-TARF aiming to achieve:

Reliability of end-to-end communication: Reliability of end-to-end communication relies on the fact that the packets initiated by the active nodes of WSN are reaching to the base station successfully. For calculating reliability there will be three situations which needs to be considered, first when the nodes are not in the direct reach of base station means they take help of intermediate nodes to complete the data packet transmission, second the nodes are in the direct reach of base station in one_hop and lastly there may be the combination of first and second case. Now the reliability can be denoted in terms of the probability of the performance of each node in WSN towards end-to-end communication under various situations.

Throughput: The ratio of total data packets reached base station to the total sampled data packets is known to be the throughput. Here we compute throughput over the interval (0,t], where 0 is the beginning time and t is the particular moment upto which data delivery happen and considered. Replicated packets due to point-to-point retransmission are termed as single packet with respect to the calculation of throughput. Effective collection and delivery of data denotes the efficiency of network through throughput. Achieving high throughput and packet delivery ratio are our main objectives.

Energy Efficiency: In WSNs major amount of energy is consumed during data transmission. Here we compute energy efficiency as average energy cost of successfully delivering unit sized data packet to base station from source. Significant increase in the energy consumption took place because of link level retransmission so it should be given sufficient focus. If nearby same energy is consumed by nodes of network then another metric hop per delivery can be used to compute the energy efficiency. In this case the consumption relies on the number of one hop transmission taking place. Measuring the average hops for delivery of each data packet we can compute the efficient energy utilization.

IV. DESIGN OF TRUSTWORTHY ROUTING FRAMEWORK USING HCF

4.1 OVERVIEW

Before node of network decides its potential neighbour which can forward the data packet to base station we would like to highlight on the component which is placed on the top of TARF model that is hop_count_filter (HCF). HCF is mainly used to categorize and detect the spoofed and non-spoofed packets. Usually spoofed packets cause serious damage to the resources of the network which may then divert the traffic. Here the hop_cnt present in packet as shown in fig. 2 will be matched with the count present in the node. Procedure followed for recognizing the spoofed and non-spoofed packet is detailed in section 4.4. Spoofed packets are simply discarded so as to protect network from unnecessary resource consumption and diversion.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Whereas on the favourable match only the packet is forwarded to the energy recorder for estimating the energy value of the potential neighbouring node as depicted in fig. 3. Logic for calculation of energy cost is described in section 4.5. Then trust_advisor is initialized for computing the trust value for the node which has initiated that packet. Computation of the trust value is explained in the section 4.6 in more detail.

Then the potential neighbour of the node is decided to route data packet by accounting the value of trust and energy. After the delivery of data packet to this next-hop node, then it will be its responsibility to send that data packet to the base station. In this case source node S_n does not know that which are the next routing decisions the next-hop is taking. For some known neighbouring nodes, S_n maintains the neighbourhood table consisting of trust,

energy and hop_cnt values about them. Mainly there is a need to exchange two routing information in addition to the data packet transmission. First is data delivery information of broadcast message from base station and second is report of energy cost. None of these messages require acknowledgement. The overall network is flooded by base station's broadcast message. SSN is used to check the freshness of broadcast message. Neighbours will get the energy cost report only once by each node. This information is not forwarded by any neighbouring node and it is only for information and record.

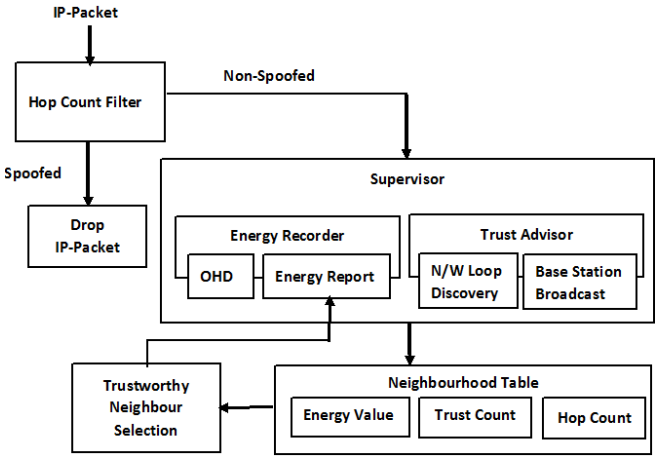


Figure 3: System architecture of M-TARF.

Data packet validity is been checked by the component HCF. Trust_advisor and energy_recorder are the two components responsible for maintaining neighbourhood table holding trust and energy values about certain known neighbours on the basis of its observation of its reachability in single hop to its neighbours and the energy cost report from them. Adversaries may publicise themselves among the member node and insist them to select it as next forwarder. But the trust_advisor track the low trust of this compromised node and the member nodes certainly avoid this compromised next-hop node to be selected as forwarder. Responsibility of trust_advisor is to track the level of trust of neighbours on the basis of discovery of loop and base station's broadcast message about data delivery. As per the neighbourhood table if S_n is able to choose its next-hop node, S_n will send its energy cost report and broadcast to its every neighbour to deliver the packet to base station. This type of report also work as input to its receiver's energy recorder.

4.2 PROCESS OF ROUTING

Like other routing schemes, M-TARF also run as periodic service. Frequent routing information exchanges and updates are been determined by the length of these periods. At the start of every period, broadcasting of data delivery message of some contiguous packets to the overall network is done by base station. Each of these packet holds the status that how may packets are remaining to complete the broadcast of current message. Exchange of energy report involved as soon as base station completes its broadcast in this new period. After the reception of this message the member node understand the end of current period and the start of new period. As stated earlier there is no need of tight time synchronization for member nodes to track this starting and end of period. In every period, the energy_recorder running on a node observes consumption of energy of one_hop packet transfer to neighbours and then maintain the energy value in the neighbourhood table with the help of energy_cost reports processed by receiver which is one_hop neighbour. At the same time trust_advisor observes the network loop and maintains trust_values in neighbourhood table based on the processing of those messages concerning data delivery. To keepup the steadiness of routing path, a member may continue with the same next_hop node till the next new message broadcast by base station arrives. Concurrently, to reduce traffic, the report of its energy_cost can be setup so that it will not take place until next new broadcast form base station. In this case if nodes doesn't change its next_hop node selection, that ensures loop-free path. But due to complexities because of calculation and waiting will results in resistive refinement of routing paths. So in our implementation, node is allowed to select new next_hop in a period at which the poor reception and delivery of data is performed by current next_hop node.

Base station broadcast message accommodated into fixed small number of packets. This message holds the pair of $[Source\ id, Seq\ No\ \{a,b\}\ length\ undelivered]$, $[Source\ id, last\ period's\ min\ and\ max\ sequence\ no]$, along with node id intervals without any delivery record in last period. To significantly reduce the overhead in our implementation we select few such pairs to broadcast. Traffic is diverted by adversaries stealing identity of nodes and mislead them with great possibility. SSNs are analysed by base station to check which SSNs corresponding to source node having that identity, are absent and select definite notable interval $\{i,\ j\}$ of these absent SSNs are referred as undelivered sequence intervals. Suppose base station has SSNs for source node 11 as $\{58, 59, 60, 91, 92\}$ in the latest previous cycle. So $\{61,\ 90\}$ is the undelivered sequence interval, also $\{58,\ 92\}$ is noted as the boundary for packets which are delivered.

Every node of the network maintains table having source node id, sequence interval forwarded $\{u,\ v\}$ with length of last cycle. SSNs falling under $\{u,\ v\}$ are already forwarded by this node. After the reception of broadcast message from base station node's trust_advisor will identify the not delivered but forwarded data packets to base station. To consider and reduce overhead to maintain such table and to keep it manageable the old entries are removed once it is full. The existing energy_value entries are immediately abundant by the node as soon as it receive a fresh message broadcasted by base station and it will be ready to receive fresh report from neighbours and select its new forwarder.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Node selection is carried by it either after timeout or after reception of energy report from trusted neighbours with appropriate energy cost. Once next_hop node is decided by node, immediately it will broadcast its energy_value to neighbours. Calculation of energy_value of node to next_hop node is discussed in section 4.5. There may be ambiguity in knowing that which node will broadcast energy_report first. Base station broadcast is understood as energy_report by neighbouring node receiving that message as base station to reach itself require no energy. Base station will be considered as faithful provided that it is original and trustworthy by trust_advisor on its neighbours. Hence those neighbours are the first to determine their next_hop node and the base station and after that decision is over they will start reporting their energy_value.

4.3 ROUTE SELECTION

In this section we discuss and introduce the process of M-TARF follows to decide routes in WSN. Every node relies on its neighbourhood table to choose the optimal route by considering the expenditure of energy and trust. M-TARF makes a reliable attempt to avoid adversaries misdirecting routing by replaying routing information.

To select the route to deliver data to base station node A will select an ideal next_hop node amongst its neighbours on the basis of trust and energy values and immediately forward the data packet to that next_hop node. If the trust_value of neighbours falls below fixed threshold then those node will be kept aside of route. Form the known neighbours left, A will select its next_hop by assessing each neighbour B on the basis of trade_off between T_{AB} and E_{AB} / T_{AB}, where T_{AB} and E_{AB} are trust and energy_values in neighbourhood table respectively. Assuming each node in the route is ideal and honest, E_{AB} denotes the energy value to deliver a packet to base station. Inverse of T_{AB} indicates the no of required trails to send packet to base station through multiple hops prior to the success of trail, taking into account the trust value of B. Hence for the efficient and correct packet transmission energy_value should be low with higher trust_value with respect to next_hop node. So E_{AB} / T_{AB} have both these crucial parameters that is trust and energy_value.

An attacker may wrongly report with sufficiently low energy_value to divert traffic through it, so even with low T_{AB} the overall metric E_{AB} / T_{AB} is badly affected by these attackers. To avoid this situation nodes with significantly high trust values are preferred and this approach efficiently shield the network by attackers stealing identity of node with highest attention such as base station.

4.4 HOP COUNT COMPARATOR

There are many mechanisms to handle Denial of Service, for our proposed implementation our main focus is on Hop Count Filtering Technique. In the existing model of TARF, a new component called Hop Count Comparator is introduced. This component is responsible for comparing the standard hop count from a mapping table in each node to the actual hop counts obtained from the packet. This technique helps to distinguish between spoofed and non-spoofed packets. The legitimate packet would be handed over to the energy recorder to determine the next hop whereas the spoofed one will be simply discarded. In this way, this technique will defend WSNs against DoS[2].

Let x are the total number of attempts HCF makes to compare packets initiated. Classification of packets whether they are spoofed or non-spoofed let y is the intermediate attempt that HCF makes to compare hop_count for all packets initiated. Then x can be expressed as $x = (x \cap y) \cup (x \cap \bar{y})$ then the corresponding probability in general for y_i such comparisons using the theorem of total probability will be

$$P(x) = \sum_{i=1}^{n} P(x|y_i)P(y_i) \quad \ldots\ldots\ldots 1$$

With the probability of occurrence of x it is not possible to identify that whether packet is spoofed or non-spoofed. Suppose $y_1, y_2, y_3, \ldots\ldots\ldots y_j$ are mutually exclusive event of success in every attempt. Then for declaring the packet is successfully traced as non-spoofed our aim is to calculate the probability of occurrence of y_j against the overall attempts x i.e. $P(y_j|x)$ which is $Success_{HCF}$. By using the concept of conditional probability, which is the effectiveness of HCF for j packets to be successfully declared as non-spoofed so that it can be processed further to energy_recorder. Further $Success_{HCF}$ can be expressed using eq. 1 in simplified way as

$$Success_{HCF} = \frac{P(x|y_j)P(y_j)}{\sum_{i=1}^{n} P(x|y_i)P(y_i)} \quad \ldots\ldots\ldots 2$$

Algorithm 1 Functionality identifying the packet is spoofed or non-spoofed.

Perform for every packet:
Final Time_To_Live $= T_{fin}$
Obtain source_node_IP address S_IP
Observe initial Time_To_Live $= T\_in$
Calculate Hop_Count$(HC) = H_{in} - H_{fin}$
Obtain Stored_Hop_Count $= H_{strd}$
Check if $HC = H_{strd} \wedge 0 < Success_{HCF} \leq 1$
Legitimate Packet: Forward to Energy Recorder
Else
Packet is Spoofed: Discard

4.5 ENERGY RECORDER

In this section it is discussed that how node $A's$ energy_recorder calculates the energy value E_{AB} for its neighbour B in its neighbourhood table and $A's$ decision on its own energy E_A. Prior to the further elaboration following are some notations which are used in next calculation:

E_{AB} is the average energy value of successful delivery of unit_sized data packet from A to base station having B as its next_hop which is responsible for further route, it may happen upto the reception of acknowledgement or the number reaches to threshold while computing E_{AB}, one-hop-transmission cost must be considered, it is the $Retransmission_{One-hop}$. $E_{A\to B}$ is the average energy cost of successful delivery of data packet from A to its neighbour B in one hop and n is the number of nodes in the network.

For $0 < Success_{HCF} \leq 1$, means packet is filtered and assumed to be non-spoofed and on the above assumption the average energy cost E_{AB} can be expressed as

$$E_{AB} = E_{A\to B} + E_B \quad \ldots\ldots\ldots 3$$

In eq 3 E_B is known but there is a need to calculate the average value of successful data delivery from A to B that is $E_{A\to B}$. For calculating this factor there will be two possibilities during one hop transmission from A to B; first either the packets will be acknowledged or they are not with probabilities P_{rep} and P_{no-rep} respectively, clearly these cases are independent of each other which results them to fall in the category of sequence of Bernoulli's trail. For n known neighbours the average number of acknowledged one_hop transfer k times can be expressed as

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$OHT_k = \frac{1}{n}\sum_{k=1}^{n} k.P_{rep}^{k}.P_{no-rep}^{n-k} \quad \ldots\ldots 4$$

If E is the energy required by node A for sending a unit_sized packet once without concerning its reception then

$$E_{A\to B} = E.OHT_k \quad \ldots\ldots 5$$

Then eq 3 can be written as

$$E_{AB} = \frac{E}{P_{rep}} + E_B \quad \ldots\ldots 6$$

Now the calculation of E_{AB} completely relies on the probabilities that one-hop-transmission is acknowledged i.e. P_{rep}. As the position of nodes in WSN is not fixed so we cannot use simplified averaging technique to calculate P_{rep}. As a substitute we adopted and updated the averaging techniques used in [20]. In this the energy recorder updates P_{rep} as and when the transmission occurs from A to B on the basis of whether that transmission is acknowledged or not using bind averaging mechanism. A variable Rep with only two possible binary values 0 or 1 is used to mark the outcome of present transfer. Its value is 1 if the reply of current transmission's successful reception realized and 0 on the other case.

Given Rep and latest previous $P_{pre-rep}$, a recursive method is to utilize simply bind average of Rep and $P_{pre-rep}$ as the value of $P_{fresh-rep}$.

To explore the provision against attacks, two binding parameters $bind\_upgrade$ and $bind\_degrade$ with comparatively larger degrade and lower upgrade values respectively, the value of P_{rep} is modified as per algo 2:

Algorithm 2: Update of energy_value by imposing penalty or reward

$for\ i = 1\ to\ n$
$When\ rep = 0$
$penalty = (1 - bind\_degrade) * P_{pre\_rep}$
$P_{fresh\_rep} = penalty + (bind\_degrade * rep)$
$When\ rep = 1$
$reward = (1 - bind\_upgrade) * P_{pre\_rep}$
$P_{fresh\_rep} = reward + (bind\_upgrade * rep)$
End

Here the binary parameters $bind\_degrade$ and $bind\_upgrade$ are adjustable according to the demand of application. These defines the degree to which the performance impose reward or penalty based on algorithm 2. $bind\_degrade$ should be assigned comparatively high value in case of misconduct due to the presence of adversary, to heavily punish this misbehaviour. If transaction is unable to be declared as positive to realize favourable communication, which require more number of such transactions, then $bind\_upgrade$ should be assigned comparatively low value.

4.6 TRUST_ADVISOR

Each node in WSN is uploaded with trust_advisor initiated immediately whenever any broadcasting is happening. After receiving non-spoofed packet by HCF with $0 < Success_{HCF} \leq 1$ but still there may be problem in deciding the trusted next_hop node which will be then responsible for further transmission. To strengthen the routing process stated in section 4.2, trust_advisor of node A decides the trust_level of each neighbour on the basis of network loop discovery and base station broadcast on delivery of data packet. For $A's$ each neighbour B, T_{AB} express the level of trust of B in the neighbourhood table of A. Moderate and neutral trust_level of 0.5 is assigned to each neighbour. Respective neighbour's trust_level is updated against network loop discovery and base station broadcast about data delivery. Antiloop mechanism to be incorporated in M-TARF completely rely on the base station broadcast to determine the level of trust. Discovery of loop may only be realized when antiloop mechanism is imposed on both the components of architecture and the routing protocol integrated in it. Many existing methods incurs overhead due to the comparison of specific route cost to discard the routes which are most likely causing loops. To reduce the overhead when antiloop mechanism is absent in the existing protocol, we choose following strategy to detect loops. Trust_advisor makes use of the table which node A maintains which is $Source\ node\ id, sequence\ interval\ forwarded\ \{u, v\}$ $with\ length$. If the data packet received is already in the table then A will discard that packet along with trust_advisor on A will degrade the reputation of that next_hop node. For B as the selected next_hop node, its latest trust_value i.e. PT_{AB} of B. Like energy_recorder where we considered Rep as binary variable in the same way for holding the status of occurrence of loop we consider another binary variable N_loop. If N_loop=0 then loop discovered and if 1 then not. In the same case of update of energy_value in energy_recorder using bind averaging mechanism the logic for calculating the fresh trust_level of B i.e. FT_{AB} shown in following figure:

Algorithm 3: Trust_advisor calculating fresh trust_level

$for\ i = 1\ to\ n$
$When\ N\_loop = 0$
$penalty = (1 - bind\_degrade) * PT_{AB}$
$FT_{AB} = penalty + (bind\_degrade * N\_loop)$
$When\ N\_loop = 1$
$reward = (1 - bind\_upgrade) * PT_{AB}$
$FT_{AB} = reward + (bind\_upgrade * N\_loop)$
End

Loop is broken, as node $A's$ next_hop is changed by reducing trust_level on current next_hop when A detects loop for few times that which node to be kept responsible for this. For this, by degrading the level of trust on current next_hop will lead to breaking of loop. For detecting the nodes causing replaying routing information and misdirecting the traffic, $A's$ trust_advisor compares the entries in the stored table on A with the base station's broadcast message on delivery of data. Successful Packet Delivery Ratio (PDR) is calculated by this node that the packet is successfully delivered and forwarded by it to the total number of forwarded packets. Computation of number of successfully delivered packets which are forwarded successfully let us assume there are p packets which are successfully delivered and for the first factor of PDR we are aimed to find q packets which are successfully forwarded out of m and is expressed in terms of probability as

$$P(forward_q | delivered) = \frac{P(delivered|forward_q)(P(forward_q)}{\sum_{m=1}^{n}\binom{n}{m}P_{delivered}^{m}(1-P_{delivered})^{n-m}} \quad \ldots\ldots 7$$

Then final successful packet delivery ratio (PDR) can be expressed as

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$PDR = \frac{P(delivered|forwarded_q)(P(forwarded_q)}{\sum_{m=1}^{n}\binom{n}{m}P_{delivered}^{m}(1-P_{delivered})^{n-m}} \cdot \frac{1}{P_{TPF}} \quad \ldots\ldots 8$$

Here P_{TPF} is the probability of total number of forwarded packets by HCF. Now the final update of trust_value by trust_advisor on A is done using the following logic:

Algorithm 4: Trust_value update through PDR.

for $i = 1$ *to* n
if $PDR < PT_{AB}$ *then*
$penalty = (1 - bind\_degrade) * PT_{AB}$
$FT_{AB} = penalty + (bind\_degrade * PDR)$
else if $PDR \geq PT_{AB}$
$reward = (1 - bind\_upgrade) * PT_{AB}$
$FT_{AB} = reward + (bind\_upgrade * PDR)$
End

V.V. ANALYSIS OF ENERGY_RECORDER AND TRUST_ADVISOR

In this section we will clarify certain facts on design of two crucial components energy_recorder and trust_advisor on which node A dependent on selecting its ideal next_hop neighbour node.

As in the description in energy_recorder, a member node receive the energy report as the only information which it receives passively and is used as logic for selecting next_hop node. If this energy report is forged by adversary then it will become risk due to the false report generated or manipulated by attackers. Data delivery resistance is the major target of attacker instead of diverting packets through ineffective routes, these are the attempts of adversaries to impose attack. M-TARF lessen the effect of this attempt of attacker using trust_advisor of resisting data packet delivery. Trust_advisor on one node does not take any recommendation from trust_advisor on other node. Intention of adversary of forging energy report will be avoided by trust_advisor on that node, if a node's trust_advisor observes failure of data packet delivery several times by the base station broadcast, then next_hop is penalized by degrading its level of trust by that node and then a new next_hop which is more reliable is been elected and current next_hop is switched to this new node.

On the other hand trust_advisor recognizes adversaries with low trust_values trying to misdirect multi_hop routing, specifically those causing replay of routing information. Notable point about trust_advisor is that it does not differentiate between occurrence of attack or misbehaviour to the next_hop or further forwarder in the route. It may be injustice with legitimate and honest next_hop node as trust_advisor degrades the level of trust during the occurrence of attack elsewhere in the route and after that next_hop node. Opposed to that situation PDR is increased by trust_advisor gradually in the presence of attack trying to prevent data delivery. Usually it is difficult to detect the attacker stealing identity of legitimate node and participating in the network activity. Moreover inspite of unavoidable unfairness, node is encouraged by trust_advisor to select different route when data delivery to base station is getting frequently interrupted for the current route. However legal nodes to the attacker may correctly recognize the adversary, results of evaluation that the technique of diverting to the new route by bypassing attacker gradually improves the performance of network, even in the presence of sinkhole and wormhole attacks. To elaborate this consider the network diagram shown in fig. 4, where all the nodes are honest and uncompromised.

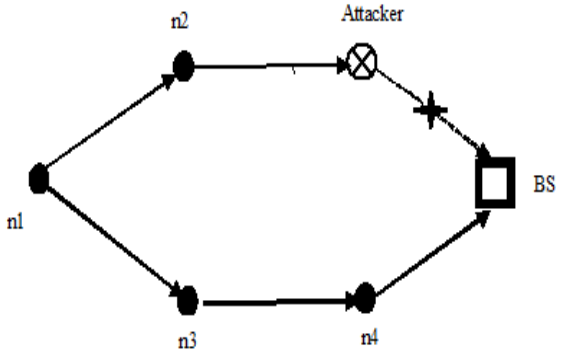


Figure 4. Working of trust_advisor which replaces the comprised route with new strong route.

Node n1 has n2 as its immediate next_hop while n2 has the attacker as next_hop. Every packet received by this attacker will be dropped. This way packets passing through n1's first route will not reach base station. After certain time node n1 comes to know that the data packets it sent is not reached base station then it start degrading the level of trust of its present next_hop node n2, however n2 is totally honest. Once the level falls below certain threshold, node n1 select n3 as its new next_hop node. In this way the attack is avoided by the trust_advisor of n1 and recognizes better route n1-n3-n4-BS. Regardless of the injustice with n2's level of trust, the performance of network will be better. Now as far as stability of route is concerned, once a legal node recognizes trustworthy honest neighbour as next_hop then it will ignore any other attractive elements such as illegal base station. This strategy is implied realize both to keep route stable and nodes highly trustable.

At the end design of M-TARF is targeted to shield WSN over the threats which mislead the multi_hop routing, precisely based on steal of identity by replay of routing information. Along with the defence against sinkhole and wormhole it also ensure defence against attacks penetrating several compromised data packets holding invalid sensing information although it is authenticated, probably because of hacking which targets to keep the network resources exhausted in place of mislead of routing. Attempt of attacker to periodically inject routing packets causing false route, this type of attack also can be defeated by M-TARF through HCF and trust_advisor.

VI. Performance EVALUATIONS

6.1 SIMULATION AND RESULT

We have developed a ready to incorporate tool which is reconfigurable and adaptable for WSN in 2-D plane on NS2 platform to observe the performance of M-TARF. We considered 100x100m rectangular area with uniform distribution of 30, 50 and 101 nodes with undependable wireless transfers, fig. 5. Same energy level and max transfer limit of 100m is assigned to every node. In each period every node sample 6 times. Same node's two consecutives sampling gap is identical. In our simulation we focused on two network topologies: first is static where in the location of all nodes including base station is fixed and other is dynamic where in the nodes are dispersed in the predefined area.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

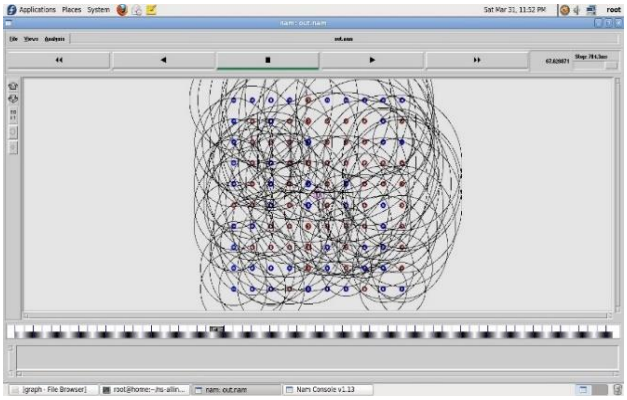
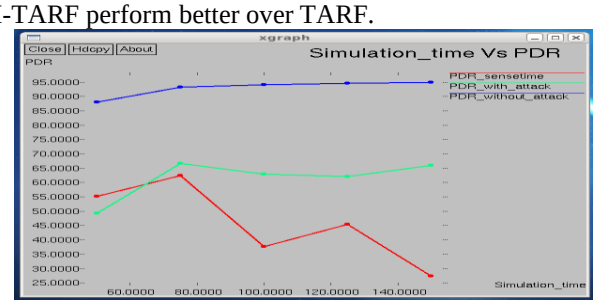


Figure 5. Nodes involved in message passing.

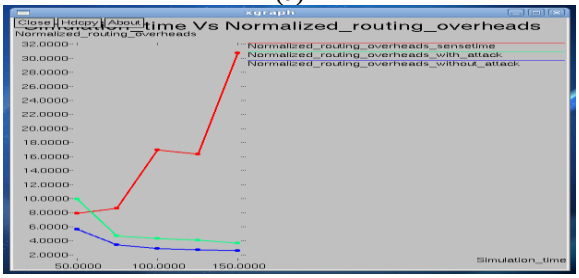
We tested our implementation in the presence of attack and without attacks, alongwith the performance measurement metric with the sensetime. The simulation results shows that our scheme outperforms in the absence of attack and in presence of attacks the throughput is significantly higher than that of TARF however hop_per_delivery is comparatively near to TARF.

Fig 6(a) shows the improved packet delivery ratio while normalized overhead and average energy consumed shown in fig 6 (b, c). For reliable end-to-end communication the packet drop ration should be minimum. In this context, the packet drop ratio in our proposed system is comparatively less as shown in fig 6(d).

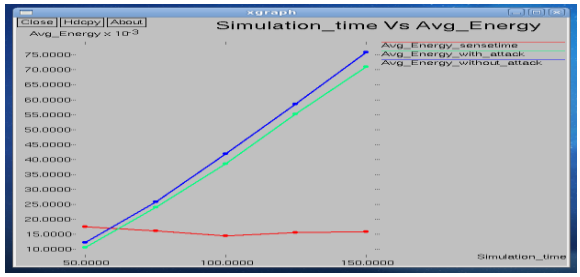
It is affordable to think of M-TARF and TARF in the scenario where no adversary is present in the network. Both of these protocols are tested against sinkhole attack in which some node steals the identity of the base station and redirect the broadcast messages, forwarding loop formation due to colliding nodes and packet drops caused by certain nodes. These evaluation is done in the case where the location of nodes are fixed. Usually in presence of above mentioned attacks, M-TARF proves improvement over TARF and other related protocols as far as throughput is concerned. Next we have evaluated M-TARF in the presence of more severe attack i.e. Sybil which is trying to create trail of false base stations, however in the presence of these two serious attacks M-TARF perform better over TARF.



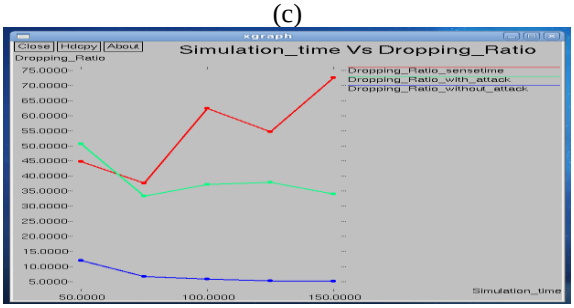
(a)



(b)



(c)



(d)

Figure 6: Performance of M-TARF with respect to sense time. Moreover another type of attack which is trying to devastate the network functionality by continuously keeping network resources busy and resisting or delaying legitimate and crucial operations to be performed by network. In our evaluation it is observed that upto great extent M-TARF successfully defend WSN against this attack where TARF fails.

But if this attack is initially launched in distributed manner by adversary then it will be out of the scope of M-TARF. At the end as per the experiments carried out on deciding the length of period and technique to update trust it is found that short period for fast trust update technique might not certainly benefit M-TARF.

6.2 COMPARATIVE ANALYSIS

The performance evaluation of MTARF is done in two cases, the first is reliability of end-to-end communication and then throughput which is the ratio of total packets reached successfully to the total packets initiated. Reliability can be evaluated in three cases, firstly where every node is directly not reachable to base station in one_hop, secondly nodes are directly reachable in one_hop and lastly some nodes are directly in range for one_hop transmission to base station where as others follow multi_hop transmission.

In case where nodes follow multi_hop routing, suppose R_{MHTi} is the reliability of node i initiates the packet and is reaching to the base station with the help of intermediate nodes then in this case the reliability of end-to-end communication can be expressed in terms of the probability that every node of network is performing upto the mark then R_{MHT} for j legitimate node can be expressed as

$$R_{MHT} = \prod_{j=1}^{n} P(MHT_j) \qquad \ldots\ldots\ldots 9$$

In the other two cases it is mostly not possible in the WSN like adhoc network to realize direct connectivity of the nodes with the base station for data transfer. So in our discussion we consider that the nodes take help of intermediate nodes to forward the initiated data by source node.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Assessment of Throughput: Now for assessing throughput the task is to observe the transmission and reception of packet that is the ratio of total packets reached successfully to the total packets initiated inside WSN for the finite time interval $(0,t]$. Suppose ωt is the small interval belong to the mentioned fixed time interval, then the of packet to be successfully received at ωt can be written as

$$P_j(\omega t) = \mu.\omega t \qquad \ldots\ldots\ldots 10$$

Here μ is the constant and its value depends on the number of nodes n active in WSN taking part in data packet transfers. Important point to note that if ωt is very small then the probability of two or more packets received at interval of this can be neglected. For computing the throughput our aim is to calculate the probability of k packets received successfully in duration t i.e. $(0,t]$. For this purpose we have to divide this interval into small fraction and observe the same on each subinterval. Suppose there are S_i subintervals of $\frac{t}{S_i}$ length and the reception of packet in any subinterval is independent of the reception on other interval. For significantly large n the intervals form a sequence of independent transmissions with success probability as $\mu.\frac{t}{S_i}$

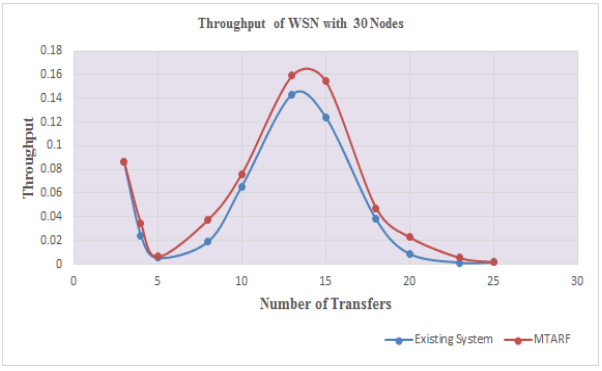
Then the throughput of k packets received in a total of S intervals each with duration $\frac{t}{S_i}$ can be given as

$$T_{Overall} = \binom{n}{k} \left(\frac{\mu t}{S_i}\right)^k \left(1 - \frac{\mu t}{S_i}\right)^{n-k} * R_{MHT} \qquad \ldots\ldots\ldots 11$$

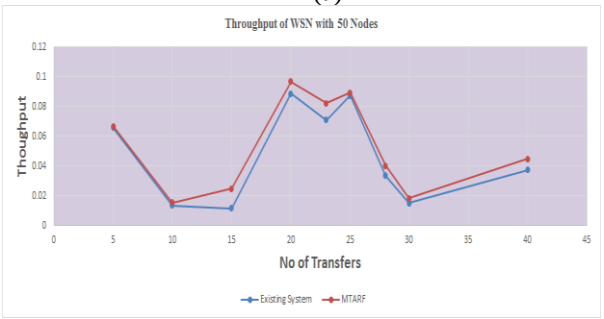
Throughput of the networks by considering active and passive nodes, eq. 11, due to which accurate approximation cannot be observed. To realize better approximation it is further simplified to evaluate final throughput that k packets successfully received out of all packets initiated by the active nodes as

$$T_{active} = e^{-\sigma} \frac{\sigma^k}{k!} * R_{MHT} \qquad \ldots\ldots\ldots 12$$

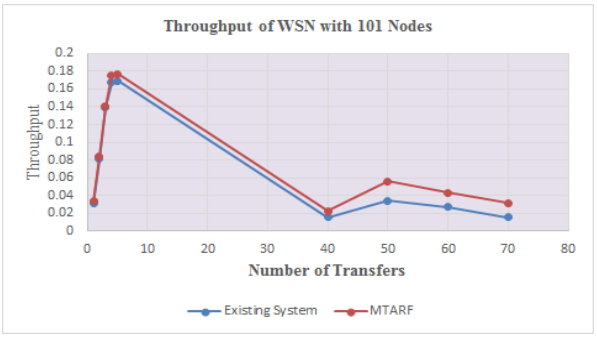
Figure 7 shows the performance improvement in terms of throughput for secured end-to-end communication between source and basestation.



(a)



(b)



(c)

Figure 7. Comparative analysis of network in presence of Sink hole and replay of routing information under densities a) 30 b) 50 c) 101

Throughput in terms of the effective end to end communication of the network is analysed with densities 30, 50, and 101. It is observed that as the density of the network get increased, better approximation is obtained. So it is clearly understood that by adding the component HCF on the top of the existing TARF model, termed as existing system in fig. 7, replaying routing information is avoided which could cause a serious damage to the network resources.

VII. CONCLUSION

The existing trust based routing schemes are first surveyed in this papers and it is been observed that most of the schemes are based of the trust relations between the nodes which is insufficient to develop full proof routing scheme. A trustworthy routing scheme using hop count filter is presented in this paper. At the beginning stage of routing $Success_{HCF}$ is calculated on the basis of which categorization of spoofed and non-spoofed packets takes place. Supervisor in M-TARF will then take charge in storing and updating the trust_count and energy_value in the current node about its immediate neighbours by Trust Advisor and Energy Recorder respectively. Defence methods to provide security against well-known attacks during routing in wireless sensor networks is presented. Here an effort is made towards improving the throughput of WSN over TARF in the presence of severe identity deception attacks. Average throughput obtained in all rounds using the proposed routing method for varying densities of 30, 50 and 101 are 5.7%, 5.3% and 8.4% respectively. In our proposed system we have used the network topology as static, however in many real time scenarios the nodes are moving in nature. So it will be challenging task to design the routing framework for WSN having dynamic topology alongwith less control overhead.

REFERENCES

1. Rijin, I. K., N. K. Sakthivel, and S. Subasree. "Development of an enhanced efficient secured multi- hop routing technique for wireless sensor networks." Development 1.3 (2013): 2320-9801.
2. Sahu, SonaliSwetapadma, and Manjusha Pandey. "Distributed Denial of Service Attacks: A Review." International Journal of Modern Education and Computer Science (IJMECS) 6.1 (2014): 65.
3. Sen, Jaydip. "Routing security issues in wireless sensor networks: attacks and defenses." arXiv preprint arXiv: 1101.2759 (2011).
4. 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.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

5. J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in Proceedings of Aerospace Conference, 2004.
6. W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Lam, "Trust based routing for misbehavior detection in ad hoc networks," Journal of Networks, vol. 5, no. 5, May 2010.
7. T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou,C. Vangelatos, and L. Besson, "Design and implementation of a trust-aware routing protocol for large wsns," International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3, Jul. 2010.
8. Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in Proceeding of the 7th Nordic Workshop on Secure IT Systems, 2003.
9. A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), 8-11 2007.
10. Ahmed M. Abd El-Haleem1 and Ihab A. Ali, "TRIDNT: The Trust-Based Routing Protocol with Ccontrolled Degree of Node Selfishness for MANET" in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
11. Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "Fbsr: feedback- based secure routing protocol for wireless sensor networks" International Journal of Pervasive Computing and Communications, 2008.
12. H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks," Wirel. Netw., vol. 16, no. 4, pp. 969–984, 2010.
13. Zhan Guoxing, Weisong Shi, and Julia Deng. "Design and implementation of TARF: a trust-aware routing framework for WSNs." IEEE Transactions on Dependable and Secure Computing, Volume 9, Issue 2, 2012 pp 184-197.
14. Junqi Duan,Dong Yang,Haoqing Zhu,Sidong Zhang,and Jing Zhao, "TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 209436, 14 pages.
15. T. Sakthivel, R. M. Chandrasekaran, "A Dummy Packet-Based Hybrid Security Framework for Mitigating Routing Misbehavior in Multi-Hop Wireless Networks", WPC, Springer Volume 101, issue 3, 2018 pp 1581-1618.
16. Pu Gong, Thomas M.Chen, and Quan Xu, "ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks", Hindawi Publishing Corporation Journal of Sensors Volume 2015, Article ID 46993, 10 pages.
17. Dr. PadmavathiGanapathi, Mrs. Shanmugapriya. D, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks." (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
18. Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, Abdul Waheed Khan, "A trust aware routing protocol for energy constrained wireless sensor network", Telecommunication Systems, Springer January 2016, Volume 61, Issue 1, pp 123–140.
19. Gayathri Dhananjayan, Janakiraman Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", SpringerPlus December 2016
20. S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sen. Netw., 2008.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)