A Trust Aware Routing with Shortest Path Framework for Wireless Sensor Networks

N Suganthi[1], M. Chella Premiga[2] , A. SivaShanmathi[3]

Information Technology,Kumaraguru College of Technology, Coimbatore, India

[1]suganthiduraisamy@yahoo.co.in
[3]sivashanmathi@gmail.com
[2]premiga.m@gmail.com

***Abstract*— Wireless Sensor Networks (WSN) consists of hundreds and thousands of nodes which are of light weight and small size. To protect WSNs from the harmful attacks exploiting the replay of routing information, a robust Trust-Aware Routing Framework (TARF) is designed, to secure routing solutions in wireless sensor networks. TARF can be developed into a complete and independent routing protocol; the purpose is to allow existing routing protocols to incorporate our implementation of TARF with the least effort and thus producing a secure and efficient fully-functional protocol. In the existing system, various types of attacks are avoided. Also, trust and reputation management systems cannot be applied to WSNs due to the excessive overhead for resource-constrained sensor nodes powered by batteries. In our proposed system, we have added security to trust manager that protects against all kinds of attacks which are excluded in existing system. In addition, geographic location of the nodes is also found and hence we can choose the shortest path for fast delivery of the data.**

***Keywords*— Wireless Sensor Networks, Secure Routing, Trust Management, Routing Protocols, Minimum path cost.**

I. INTRODUCTION

Wireless Sensor networks (WSN) is a large network which is consist of huge number of sensor nodes and these nodes are directly interacting with their environment by sensing the physical parameters such as temperature, humidity, etc[1]. A sensor network deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing.[2]. However, the multihop routing of WSNs often becomes the target of malicious attacks. An intruder may attack nodes either physically or, refuse to forward certain messages, jam or cause collision on each forwarded packet while data transmission. The characteristics of network sensors are dense sensor node deployment, battery powered sensor nodes, severe energy, computation, and storage constraints, self configurable, unreliable sensor nodes, data redundancy, application specific, many-t-one traffic pattern, frequent topology change. WSNs are vulnerable to various types of attacks which are mainly of three types:

(i) *Network availability attacks*: attacks on availability of WSN are often referred to as DoS attacks.

(ii)*Secrecy and Authentication Attacks*: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

(iii) *Stealthy service integrity Attacks*: in a stealthy attack, the goal of the intruder is to make the network accept a incorrect data [3].

TARF focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. The adversary is capable of launching harmful and hard-to-detect attacks against routing such as *Resource depletion, selective* forwarding, wormhole attacks, sinkhole attacks and Sybil attacks on the basis of identity deception [4]..

II. DESIGN CONSTRAINTS FOR ROUTING IN WSNS

A WSN consists of a large number of sensor nodes which are inherently resource constrained. These nodes have constrained processing capability, very low storage capacity, reduced computing, radio and battery resources of sensors and constrained communication bandwidth. These limitations are due to constrained energy and physical size of the sensor nodes. Due to these constraints, it is rigid to directly employ the conventional security mechanisms in WSNs. In order to optimize the standard security algorithms for WSNs, it is necessary to be aware about the limitations of sensor nodes such as:

(i) *Energy constraints***:** Energy is the biggest constraint for a WSN. In general, energy utilization in sensor nodes can be categorized in three parts:

- energy for the sensor transducer,
- energy for communication among sensor nodes, and
- Energy for computation in microprocessor.

Thus, communication is more costly than computation in WSNs.Any message extension caused by security mechanisms comes at a specified cost. Further, higher security levels in WSNs usually correspond to more energy utilization. Thus, WSNs could be divided into various security levels depending on energy cost.

(ii) *Memory limitations:* A sensor is a tiny device with only a small amount of memory and storage space. Memory of a sensor node usually consists of flash memory and RAM. In which the Flash Memory is used for storing downloaded application code and RAM is used for storing sensor data, application programs, and intermediate results of computations. Usually there is not enough space to run complicated algorithms after loading the Operating System and application code.

(iii) *Unreliable communication:* Unreliable communication is another serious threat to sensor security. For sensor networks normally the packet-based routing is based on connectionless
protocols and thus inherently deceptive. Packets may get damaged either due to channel errors or may get dropped at highly congested nodes. Furthermore, the wireless communication channel is unreliable which lead to damaged or corrupted packets. Higher error rate also mandates difficult error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication may not be proper . This is due to the broadcast nature of wireless communication, as the packets may collide in transfer and may need retransmission.

(iv) *Higher latency in communication:* In a WSN, the multi-hop routing, the network congestion and processing in the intermediate nodes may lead to higher latency in the packet transmission. This makes synchronization highly difficult to achieve. The synchronization issues may be sometimes highly critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution.

Due to the, routing protocols in wireless sensor networks are expected to fulfil the following requirements*:*

*i) Autonomy***:** The assumption of a dedicated unit that controls the routing resources does not stand in wireless sensor networks and therefore it could be an easy to attack. Since there will not be any centralized authority to make the routing decision, the routing schemes are transferred to the nodes in the network.

ii) Energy Efficiency: Routing protocols should prolong network lifetime while maintaining a good grade of connectivity to allow the communication between the nodes in the network and therefore it is important to note that the battery replacement in the sensors is quite impossible since most of the sensors are randomly placed. Under few circumstances, the sensors are not even reachable [5].*iii) Scalability:* Wireless sensor networks are consists of hundreds or thousands of nodes so that routing protocols should work with this amount of nodes. *iv) Resilience:* Sensors may unpredictably stop operating either due to environmental reasons or due to the battery consumption. Routing protocols need to cope with this eventuality so when a current node is fails; an alternative route could be discovered.Several other featres are also considered.

III. Related Work

Trust-based enhancements on the routing protocols for WSN have been widely addressed in the literature. The most important research results in this direction include:

1) Trusted AODV: Very well-known AODV routing protocol has been extended to perform routing by taking into account trust metrics. A trust recommendation mechanism was first introduced and then the routing decision rules of AODV are modified to take into account trust. Of particular interest, a set of policies is derived for a node to update its opinions towards other nodes as it is necessary to design a trust information exchange mechanism when applying the trust models into network applications. More specifically, three procedures (Trust Recommendation, Trust Judgment, and Trust Update) are defined as well as the accompanying Route Table Extension, Routing Messages Extensions, and Trusted Routing Discovery.

2)Trajectory-Based Forwarding (TBF) [7]: TBF is a routing protocol that requires a sufficiently dense network and the presence of coordinate system so that the sensors can position themselves and estimate the distance to their neighbours. The source specifies the route to the packet, but does not explicitly indicate the path on a hop-by-hop basis. Based on the information about location of its neighbour's, a forwarding sensor makes a desirous decision to determine the next hop which is closest to the trajectory fixed by the source sensor. Route maintenance in TBF is not affected by sensor mobility given that a source route is a trajectory that does not include the names of the forwarding sensors. In order to increase reliability and capacity of the network, it is also possible to implement the multipath routing in TBF where an alternate path is just another trajectory. TBM can be used for implementation of the networking functions such as flooding, discovery, and network management. TBF can also be used for discovery of resource. Another interesting application of TBF is securing the perimeter of the network.

3)Directed Diffusion [8]***:*** Directed diffusion is a data-centric routing protocol for sensor query dissemination and processing. It meets the main requirements of

Wireless Sensor Networks such as scalability, energy efficiency, and robustness. Directed diffusion has several different key elements namely *data naming, interests and gradients, reinforcement and data propagation.* A sensing task can be described by a list of an attribute-value pairs. At the beginning of directed diffusion process, sink specifies a low data rate for all the incoming events. After that, the sink can *reinforce* anyone particular sensor to send events with a higher data rate by resending the original interest message with a smaller interval. Similarly, if a neighbouring sensor receives the interest message and finds that the sender's interest has a higher data rate than earlier, and this data rate will be higher than that of any existing gradient in the network, it will *reinforce* one or more of its neighbour's.

4)Rumor Routing [9]: Rumor routing is a logical compromise between query flooding and event flooding app schemes. Rumor routing is an efficient protocol if the number of queries is between the two intersection points of the curve of rumor routing with those of query flooding and event flooding. Rumor routing is mainly based on the concept of an *agent,* which is a long-lived packet that traverses in a network and informs each sensor it encounters about the events that it has learned during its network traverse. An agent will travel the entire network for a certain number of hops and then it will die. Each sensor, including the agent will maintain an event list that has event-distance pairs, where every entry in the list contains the event and the actual distance in the number of hops to that event from the presently visited sensor. Therefore, whenever the agent encounters a sensor on its own path, it synchronizes its event list with that of the sensor it has encountered. Also, the sensors that hear the agents update their event lists according to that of the agent in order to maintain the shortest paths to the events that occur in the network.

IV. DESIGN OF TARF

TARF is implemented to secure the multihop routing in Wireless Sensor Networks against intruders misdirecting the multihop routing by evaluating the trustworthiness of neighbouring nodes . It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve an acceptable throughput. TARF is also highly scalable, energy efficient, and well adaptable. Before introducing the detailed design, we first introduce several necessary notations here:

Fast Delivery: From every source node N, there will be several paths to reach the destination with minimum cost. Thereby, to transfer data from any node to destination the shortest path is found. If that path consists of any malicious node, then it should be eliminated and next shortest path should be choosed.The major advantage of this type of routing is fast delivery of data to all the destinations.

Neighbour: For a node N, a neighbour (neighbouring node) of N is a node which 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 N's opinion of that neighbour's level of trustworthiness. Specifically, the trust level of the neighbour is N's estimation of the probability that
this neighbour correctly delivers data received to the base station. That trust level is denoted as T throughout this paper.

Energy cost: For a node N, the energy cost of a neighbour is the average energy cost to successfully deliver a unit sized data packet with this neighbour as its next node, from N to the base station. That energy cost is denoted as E in this paper.

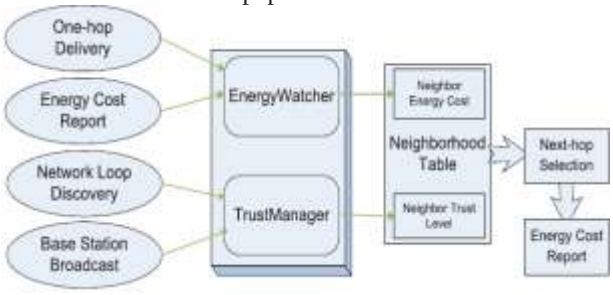

Fig.1 Each node selects a next node based on its neighborhood Table and broadcast its energy cost within its neighborhood. To maintain this neighbourhood table, Energy Watcher and Trust Manager on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbour's.

A. *Overview*

For a TARF-enabled node N to route a data packet from source to destination N needs to decide 3 main things: 1) A broadcasting message should be sent to all the nodes regarding the data transfer 2) all shortest paths from source to destination 3) to which neighbouring node it should forward the data packet considering both the trustworthiness and the energy-efficiency. Once the data packet is sent to that next-hop node, the remaining work is 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 neighbourhood table with trust level values and energy cost values for certain known neighbours. It is sometimes necessary to delete some neighbours' entries to keep the table size acceptable [10]. In TARF, in addition to data packet transmission, we exchange two types of routing information that need to be exchanged: broadcast messages from the base station about data delivery and energy cost report messages from each node. Neither the message needs to be recognized. A broadcasting message from the base station is flooded to

the whole network. The freshness of the broadcasting message is checked through its field of source sequence number. There is another type of exchanged routing information which is the energy cost report message from each node, which has to be broadcasted only to its neighbours once. Any node receiving such an energy cost reporting messages will not forward it. For each node N in a WSNs, to maintain such a neighbourhood table with trust level values and energy cost values for certain known neighbours, two components, Energy Watcher and Trust Manager, run on the node (Fig. 1).Energy Watcher is responsible for recording the energy cost for each known neighbour, based on N's observation of one hop transmission to reach its neighbours and the energy cost reports from those neighbours. A compromised node may sometimes falsely report an extremely low energy cost to lure its neighbours into selecting this compromised node as their next-hop node; however, many times these TARF-enabled neighbours eventually abandon that compromised next-hop node based on its low trustworthiness as tracked by Trust Manager. Trust Manager is mainly responsible for tracking trust level values of neighbours based on network loop discovery and broadcast messages from the base station about data delivery. Once N is able to decide its next-hop neighbour according to its neighbourhood table and then it 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. Such an energy cost report also serves as the input of its receivers' Energy Watcher. For finding the minimum distance between the nodes, the Dijktra's algorithm is made used.

B. *Broadcasting Messages*

In order to transmit data from one node to another node, via base station a broadcasting message should be sent all the nodes in the network. To save the energy of the base station, we identify the nearest nodes of the base station and forward the broadcasting message to them which is then forwarded to their nearest node and so on until it reaches all the nodes in the network. This broadcast message consists of information such as source node id, destination node id and data to be transmitted. As soon as this message reaches the source node it will begin the process of sending the data in the shortest path. Once this message is transferred to the next node it should add its own id in the path field and forward it to their next node and so on until it reaches the destination node in the network. Incase of any failure in data delivery to the destination node, the broadcasting messages has to be sent all the nodes indicating that the data transmission has not yet ended and the retransmission of messages should be started. This broadcasting message will contain data such as source id, destination id and the node at which the data transformation has been aborted.Once the data reaches the destination, the base station will send another broadcasting message to all the nodes in the above mentioned manner, indicating that the data transmission has ended and asking all the nodes to clear the information about previous data transmission. Now the network is ready for next transmission.

C. *Trust Manager*

The initialization of Node Trust Value For the sake of description, we introduce two concepts: routing node and non-routing node. Routing node is a type of next hop neighbour node selected to forward packets to the base station. Non-routing node means one of neighbour nodes except routing nodes. The credibility system mainly uses to ensure route security, therefore in order to save unnecessary expenses, the trust evaluation is only for routing nodes, however half trust attitude is adopted for non-routing nodes (that is to say that the credibility of non-routing nodes is set as 0.5). Note that non-routing node is not fixed, it is possible to become a routing node at some time, and when a non-routing node has been changed into a routing node, the system will re-evaluate the node's credibility. The working of Trust Manager is illustrated in the Fig 2

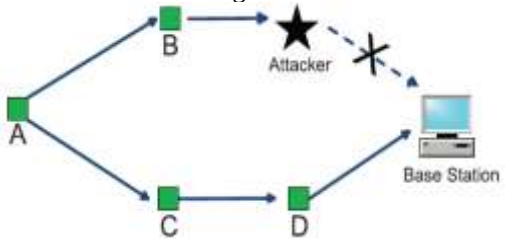

Fig.2 Asimple demonstration for Trust Manager

The goal of the trust model is to choose credible node for routing information in order to ensure the data to reach the base station safely without losing packets maliciously. The evaluation of overall validity of nodes in trust model would be involved in direct credibility and recommended credibility comprehensively (namely indirect credibility), where the previous node is concluded from direct interaction with evaluated node, while the latter is inferred from others nodes to the evaluated node. While selecting next hop node in the consideration of energy load balancing of sensor network, we will take surplus energy ratio as a standard.The trust model is based on the following assumptions: 1) WSNs is safe after initialization and 2) after routing discovery, each node stores multiple routing paths to base station. In the stage of data transmission, nodes need to select routing paths, that is to say next node. Trust value obtained from the evaluation of trust system will be a basis of route

selected, and the arbitrary node will try to choose neighbour nodes with high trust value and high energy surplus ratio as routing node. As for neighbour nodes whose trust value is lower than threshold value, the node will submit mistrust reports to base station. If base station receives the same mistrust report from different nodes to some node many times, it will exclude the node from routing table, so as to achieve the goal that the network consists of trusted nodes [11].

D. *Energy Watcher*

Another way of evaluating routing behaviour is the energy consumed while routing data packets. In this paper, we determine whether energy consumption is well balanced between the nodes. The energy metric has a major role in balancing consumption. Without the energy metric, the data packets would take the same path and deplete the energy of the nodes on that path. Here we describe how a node N's Energy Watcher computes the energy cost ENb for its neighbour b in N's neighbourhood table and how N decides its own energy cost EN.Before going further, we will clarify some notations. ENb mentioned is the average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N's next-hop node being responsible for the remaining route. Here, one-node re-transmission may occur until the acknowledgement is received or the number of retransmissions reaches a certain threshold. The cost caused by one-hop re-transmissions should be included when computing ENb. Suppose N decides that A should be its next-hop node after comparing energy cost and trust level. Then N's energy cost is EN = ENA. 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 re-transmission cost needs to be considered. With the above notations, it is outright to establish the following relation:

$$ENb = EN \rightarrow b + Eb$$

Since each known neighbour b of N is supposed to broadcast its own energy cost Eb to N, to compute ENb,N still needs to know the value EN→b, i.e., the average energy cost of successfully delivering a data packet from N to its neighbour b with one hop.

E. *Fast Delivery Of Data*

In order to perform fast delivery of data, we should find all shortest paths with minimum cost from each node to all the other nodes in that network. In order to find those shortest paths, we should be aware of the geographic location of each nodes which is quite complex to find out after fixing the sensor nodes. Hence we should note down their location while installation and calculate the distance between the nodes manually. After knowing the distance we can make use of Dijkstra's algorithm to find the minimum distance to transfer data from source to destination. For a given source vertex (node) in the graph, the algorithm finds the path with least cost (i.e. the shortest path) between that vertex and every other vertex. It can also be used for finding minimum costs of shortest paths from a single vertex to a single destination vertex by stopping the algorithm once the shortest path to the destination vertex has been determined. The algorithm is explained as below:

```
Given a graph, G, with edges E of the form (v1, v2) and
vertices V, and a source vertex, s
dist: array of distances from source to each vertex
prev : array of pointers to previous vertices
i    : loop index
F    : list of finished vertices
U    : list or heap unfinished vertices
/* Initialization: set all node's distance to INFINITY
until we discover a path */
for i = 0 to |V| - 1
   dist[i] = INFINITY
   prev[i] = NULL
end
/* The cost from the source to the itself is defined to be
zero */
dist[s] = 0
/* This loop corresponds to sending out the explorers
walking the paths, where the step of picking "the vertex,
v, with the shortest path to s" corresponds * to an
explorer arriving at an unexplored vertex */
while(F is missing a vertex)
  pick the vertex, v, in U with the shortest path to s
  add v to F
  for each edge of v, (v1, v2)
     /* The next step is at times given the confusing
name "relaxation"
     if(dist[v1] + length(v1, v2) < dist[v2])
        dist[v2] = dist[v1] + length(v1, v2)
        prev[v2] = v1
        possibly update U, depending on implementation
     end if
  end for
end while
```

V. IMPLEMENTATION

In the MATLAB implementation, a random network of 50 nodes was created and Dijkstra's algorithm was used to find the shortest routes between Source node and destination node. Then each node is evaluated for its trustworthiness and energy efficiency in the chosen path using Trust Manager and Energy Watcher. Then, the data is forwarded through that path. If there is any malicious node in that path, then the data is sent through the previously calculated next immediate shortest path.

We have evaluated three common types of attacks : 1) a certain node forges the identity of the based station by replaying broadcast messages, also known as the sinkhole attack; 2) a set of nodes colludes to form a forwarding loop; and 3) a set of nodes drops received data packets. All these attacks are prevented successfully in our paper.

VI. FUTURE WORK

This mechanism is currently a work in progress. We have only added the feature of fast delivery of data by finding the paths with minimum cost in this protocol. We have yet to define a way to add additional security in routing by securing the data that is transmitted. We have planned to ensure the data security by using the following three different ways: *Disk Encryption:* It refers to encryption technology that encrypts data on a drive. Disk encryption typically accepts form in either software or hardware. Disk encryption is often mentioned to as on-the-fly encryption ("OTFE") or transparent encryption. *Backups:*They are used to ensure data which is lost can be recovered.*Data Masking:* Data masking of organized data is the process of masking specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel.

VII. CONCLUSION

WSNs impose new challenges on the design of security tools which are more imperative than ever due to their unattended operation in open environments. To protect against routing attacks, the implementation of a trust management system is suggested. With the idea of trust management, the TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a route. Not only does TARF circumvent those malicious nodes misusing other nodes' identities to misdirect network traffic, it also accomplishes efficient energy usage. Our implementation and simulation results indicate that

1) Based on the unique characteristics of resource-constrained WSNs, the design of TARF centers on energy efficiency and trustworthiness. TARF module proves low overhead.2) TARF requires neither tight time synchronization nor known geographic information. TARF proves resilient under various attacks exploiting the replay of the routing information, which is not achieved by existing security protocols.

3) Even under strong attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks, and hostile mobile network condition, TARF demonstrates steady improvement in network performance.

REFERENCES

[1] Meenakshi Diwakar and Sushil Kumar, "An Energy Efficient level based Clustering Routing protocol for Wireless Sensor Networks "International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.2,(2012)

[2] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho," Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" IEEE Transactions On Network And Service Management, VOL. 9, NO. 2, (2012)

[3] Guoxing Zhan, Weisong Shi, and Julia Deng," TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks" Springer-Verlag Berlin Heidelberg (2010)

a. Jaydip Sen," Routing Security Issues in Wireless Sensor

[4] Networks: Attacks and Defenses" Innovation Lab, Tata Consultancy Services Ltd.India (2010)

[5] Luis Javier García Villalba , Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas," Routing Protocols in Wireless Sensor Networks" Sensors, ISSN 1424-8220,(2009)

[6] X:u, j. Heidemann, and d. Estrin, "Geography-Informed Energy Conservation For Ad-Hoc Routing", Proceedings Acm/Ieee Mobicom'01, Rome, Italy, pp. 70-84(2001).

[7] B. Nath, D. Niculescu, "Routing On A Curve", Acm Sigcomm Computer Communication Review ,Vol. 33, no.1, pp. 155-160(2003).

[8] C. Intanagonwiwat, R. Govindan, D Estrin, "Directed Diffusion: A Scalable And Robust Communication Paradigm For Sensor Networks", proceedings acm mobicom'00, Boston, (2000).

[9] D. Braginsky,D. Estrin, "Rumor Routing Algorithm In Sensor Networks", Proceedings Acm Wsna In Conjunction With Acm Mobicom'02,atlanta, pp. 22-3 1(2002).

[10] Guoxing Zhan, Weisong Shi, Julia Deng," Design And Implementation Of Tarf: A Trust-Aware Routing Framework For Wsns, IEEE transactions on dependable and secure computing, vol. 9, no. 2, (2012)

[11] Research On Beta Trust Model Of Wireless Sensor Networks Based On Energy Load Balancing

[12] N. Pushpalatha1, Dr.B.Anuradha2 "Shortest Path Position Estimation Between Source And Destination Nodes In Wireless Sensor Networks With Low Cost., International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2,(2012)

[13] Xiumin Wang, Jianping Wang Kejie Lu, "Gkar: A Geographic K-Any cast Routing For Wireless Sensor Networks" ieee transactions on parallel and distributed systems,(2012)

[14] Mat lab, http://www.mathworks.com