Reliable Opportunistic Adaptive Routing in Wireless Sensor Networks in Contradict to Denial of Service

Pritesh A. Patil[1] Prachi Bhagwat[2] Neha Kumari[3] Shagufta Shaikh[4]
[1]Head of Department [2,3,4]Student of B.E
[1,2,3,4]Department of Information Technology
[1,2,3,4]AISSMS IOIT, Pune, India

Abstract— Wireless Sensor Networks sends data from sender to base station using number of sensors. However, the multi hop routing of WSNs often becomes the target of malicious attacks. Traditional cryptographic-based security mechanism have proved to be ineffective against several hard-to-detect insider attacks such as wormhole attack, sinkhole attack, sybil attack, selective forwarding attack, etc. These attacks further produce severe impacts on replaying of routing information and also aggravate identity deception. Present routing algorithms and protocols could not solve these severe problems. For such circumstances, TARF can be used to provide a trustworthiness and energy efficient route without any known geographic information or tight time synchronization. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and networks. Other WSNs related problem is Denial of Service which is caused by many popular attacks. DoS attacks are complex and serious problem affecting not only a victim but the victim's legitimate clients as well. TARF provides protection against above mentioned attacks but fails to ensure protection against DoS. In our proposed system, we make an endeavour to introduce a mechanism to tackle DoS attacks on the wireless sensor network which would further strengthen its security in all aspects.

Key words: WSNs, TARF-Trust aware routing frameworks, DoS-Denial of Service, Sybil attack, sinkhole attack, wormhole attack

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are emerging networking technologies for low-cost, unattended monitoring of a wide range of environments. A WSN typically consists of tens, hundreds, or even thousands of low-cost, low-power, and multifunctional sensor nodes that are deployed in a region of interest. WSN can be well illustrated with the figure below. These tiny sensor nodes are equipped with sensing functionalities, embedded microprocessors, radio transceivers, and small memory. They communicate over a short distance wirelessly and cooperate to accomplish a common task, such as environmental monitoring.

Recently, Wireless Sensor Networks (WSNs) have been deployed into a variety of applications including homeland security, military systems, and health care. Sensor nodes deployed in such networks are subject to several attacks such as sinkhole and select forwarding, wormhole, Hello flood, and replication attacks. Therefore, developing secure and energy-efficient routing protocols to protect WSNs against these attacks while efficiently utilizing the energy of the deployed nodes has become imperative. Several routing protocols have been proposed for WSNs. Most of these protocols assume static nodes and sinks to collect data from network fields. However, they may be highly movable, and recent advances show that mobile sensors in WSNs have a promising performance. Therefore, this paper surveys the state of the art on routing protocols related to WSNs and presents the security issues or problems associated with the current protocols as well as discuss a secure trust aware routing framework providing secured transmission of packets resistant to most of the attacks.

The remainder of the paper is organized as follows:

The second section describes the background of the Wireless Sensor Networks. It describes the several attacks on the WSNs. The third section describes defines the goal of the proposed system. The fourth section gives a detail view of the proposed system. It describes the block diagram and several modules associated with the proposed system. The fifth section details the protocols used in the system.

The sixth section gives implementation details with the screen shots of the system.

A. Applications of WSNs:

WSNs are currently being employed in a variety of domains ranging from commercial, industrial, environmental, and healthcare to military applications to monitor data that would be difficult or expensive to capture using wired sensors. Based on these fields, a variety of applications have been presented in the literature including aircraft monitoring, ecological habit monitoring, and geological monitoring. Wireless biomedical sensor networks (WBSNs) are another application domain for WSNs that is characterized by the necessary low error rates compared to traditional WSNs. Another trend in the WSNs applications is the Vision- Enabled Wireless Sensor Networks which is a new application platform for Wireless Image Sensor Network. Application examples of this category include Event Detection, Multimodal Node Localization, Collaborative Self-Localization, Traffic Monitoring, and Target Tracking. [5]

B. Literature Survey:

WSNs have some special characteristics that distinguish them from other networks such as the Internet. The characteristics, listed as follows, demand careful considerations for protocol and algorithm

Designs that can lead to the use of WSNs in the real world:

- Sensors have limited resources, such as energy, memory and computation capacity. Light-weight protocols and algorithms are referred to achieve longer sensor life.

- Sensors have limited reliability, partially because of the resource constraints.
- WSNs usually have dynamic topologies. Aside from sensors' leaving the network for reliability issues, new sensors may be added or activated and join the WSNs.
- WSNs can well have a large number of sensors.
- WSNs are usually centralized in terms of data processing and sometimes control as well. Data flow from sensors towards a few aggregation points which further forward the data to base stations of a fewer number. Base stations could also broadcast query/control information to sensors.

Unfortunately, most existing routing protocols for WSNs assume the honesty of nodes and focus on energy efficiency, or attempt to exclude unauthorized participation by encrypting data and authenticating packets. Examples of these encryption and authentication schemes for WSNs include TinySec, Spins, TinyPK, and TinyECC.[1]

Thus making Wireless sensor networks more vulnerable to malicious attacks. It is very crucial to incorporate security mechanisms to protect the important data being transmitted over the network. In the existing system it is done by incorporating several overheads and costly mechanisms thus making it infeasible. Our proposed system makes an endeavour to tackle several attacks and strengthen the wireless sensor networks with limited overhead and cost effective method. Our focus is on routing security in wireless sensor networks.

II. BACKGROUND

We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed to monitor and affect the environment.

Sensor networks often have one or more points of centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage centre, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. In some previous work on sensor network routing protocols, base stations have also been referred to as links.

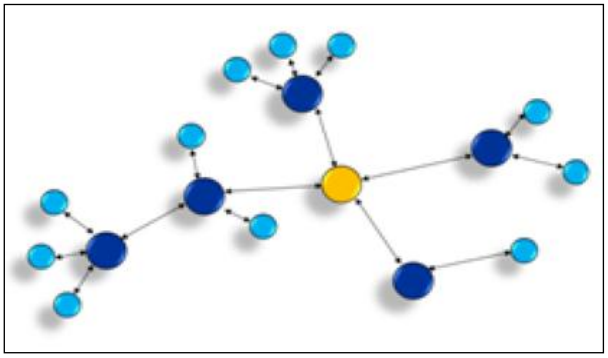

Fig. 1: An illustration of Wireless Sensor Network Architecture

A base station might request a steady stream of data, such as a sensor reading every second, from nodes able to satisfy a query. We refer to such a stream as a data flow and to the nodes sending the data as sources. In order to reduce the total number of messages sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible aggregation points. An aggregation point collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values.

Most traffic in sensor networks can be classified into one of three categories:

(1) Many-to-one: Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.
(2) One-to-many: A single node (typically a base station) multicasts or floods a query or control information to several sensor nodes.
(3) Local communication: Neighbouring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighbouring nodes or unicast messages intended for only single neighbour. [5]

A. Attacks on WSNs:

Many sensor network routing protocols are quite simple, and for this reason are sometimes susceptible to attacks from the literature on routing in ad-hoc networks. Some of the attacks are:

1) Wormhole Attack:

In this type of attack, the malicious node forges the identity of the nodes and use identity to participate in the network route, disrupting the network traffic. The routing packets, with their original header are replayed without any modification. When the packet in the routing network is send far away from the original node is called as Wormhole attack. [6]

2) Sink Hole Attack:

In a sinkhole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets. [3]

3) Sybil Attack:

In this attack, an attacker may present its multiple identities to the network while replaying the routing information. It performs same as sinkhole attack thus through replaying the routing information of multiple legitimate nodes; an attacker may present multiple identities to the network. [5]

4) Denial of Service:

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. [4]

III. GOALS

The goals of the proposed system are as follows:

1) Implement the TARF as a ready-to-use module with low overhead and easy to use in existing routing protocols.

2) Detection of and Defence against DoS attack 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. Based on the unique characteristics of resource-constrained WSNs; the design of TARF centres on trustworthiness and energy efficiency. These will be further elaborated in later sections.

IV. PROPOSED SYSTEM

This Paper targets at secure routing for data collection tasks, which are one of the most fundamental functions of WSNs. In a data collection task, a sensor node sends its sampled data to a remote base station with the aid of other intermediate nodes. Though there could be more than one base station, our routing approach is not affected by the number of base stations; to simplify discussion, assume that there is only one base station.

Some necessary concepts of TARF first we need to understand are:-

(1) Neighbour: For a node N, a neighbouring node or a neighbour of N is a node that is reachable from N with one-hop wireless transmission. [1]
(2) Hop Count Comparator: This component is responsible for comparison of standard hop count stored in mapping table to the actual hop count obtained for checking whether the transmitted packet is spoofed or not.
(3) Trust Value: 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. The trust level of the neighbour is N's assessment of the probability that this neighbour correctly delivers data received to the base station. [1]
(4) Energy Level: 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-hop node, from N to the base station.[1]

A. Block Diagram:

In TARF the source node only need to decide the next trustworthy and energy efficient neighbouring node for forwarding the data packet. Once the data packet is forwarded to that neighbouring node, the remaining task to deliver the data to the base station is fully assigned to it, and N is totally innocent of what routing decision its next-hop node makes.

The node N maintains a one table which contains attributes as trust level values and energy cost values of certain known neighbours. It is sometimes necessary to delete some neighbour's entries to keep the table size acceptable. In addition to data packet transmission, from each node the broadcast messages from base station about data delivery report as well as energy cost report messages need to be estimated. A broadcast message from the base station is flooded to the whole network. The broadcast message is checked through its field of source sequence number. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbours once. Any node receiving such an energy cost report message will not forward it.

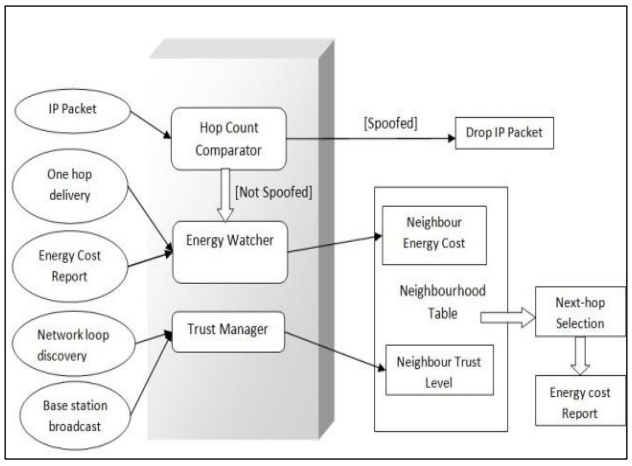

Fig. 2: Block Diagram of TARF

V. COMPONENTS

A. 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 will be introduced. This module will be 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 watcher to determine the next hop whereas the spoofed one will be simply discarded. In this way, this technique will defend WSNs against DoS. [4]

B. Energy Watcher:

Energy cost is denoted as E, sender node as N and next-hop node as b. Here we describe how a sender node'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 or destination node, with b as N's next-hop node being responsible for the remaining route. Here, one-hop re-transmission may occur until the acknowledgement is received or the number of re-transmissions reaches a certain threshold. The cost caused by one-hop retransmissions 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 retransmission cost needs to be considered. With the above notations, it is straightforward to establish the following relation: ENb = EN!b + Eb.

C. Trust Manager:

Trust in WSNs is the credibility of a node with respect to another. Reputation is the credibility of a node with respect to a group of other nodes. Trust can be defined as the degree of belief about the future behaviour of other entities, which is based on one's past experience with and observation of

their actions. Survival of a WSN is highly dependent upon the cooperative and trusting nature of its nodes.

Trust in WSN networks plays an important role in constructing the network and making the addition and/or deletion of sensor nodes from a network, due to the growth of the network, or the replacement of failing and unreliable nodes very smooth and transparent. The creation, operation, management and survival of a WSN are dependent upon the cooperative and trusting nature of its nodes, therefore the trust establishment between nodes is a must. However, using the traditional tools such as cryptographic tools to generate trust evidence and establish trust and traditional protocols to exchange and distribute keys is not possible in a WSN, due to the resource limitations of sensor nodes. Therefore, new innovative methods to secure communication and distribution of trust values between nodes are needed. Trust in WSNs, has been studied lightly by current researchers and is still an open and challenging field.

VI. PROTOCOLS

Proposed system is divided into 2 modules:

1) Routing Algorithm SOAR incorporated with TARF
2) Hop Count Comparator

A. Routing Algorithm SOAR:

Various traditional routing algorithms use a pre-determined path to route a packet from source to destination. However due to the unreliability of node arrangement in Wireless sensor nodes these algorithms prove inefficient.

Opportunistic routing is different from the traditional routing schemes in that it exploits the spatial diversity and broad cast nature of the wireless medium. It also differs in its route selection after packet transmissions i.e. forwarders of a packet are chosen amongst the recipients after the packets transmission. These features allow opportunistic routing to unite several weak links into a strong one as well as take advantage of unanticipated long or short transmission, thus allowing coping well with the unpredictable wireless medium. [2]

The Simple Opportunistic Adaptive Routing Protocol is as follows:

final forwarding list ()
for i = 1: num_nodes,
  min ETX virtual = inf,
  for j = 1: max forwarders,
    if forwarders exist i.e. forwarding list is not 0
      ETX virtual = ETX (current node, candidate node)
      Virtual link threshold = 20 (set globally)
      if matrix (current node) sum ETX + ETX virtual <virtual link threshold
        {add candidate forwarder to find forwarding list of current node}
        current node sun ETX = current node sum ETX+ETX virtual
      else
        replace the last forwarder added to the final list with the forwarder which has min ETX to current node(not destination)
      end
    end
  end
end

B. Hop Count Comparator:

In this proposed system, this module will be using the Hop Count Filtering Technique.

The Hop Count Comparator Algorithm is as follows:

1) For each packet:
2) Extract the final TTL Tf;
3) Extract source IP address S;
4) Find Initial TTL Ti;
5) Find Hc (Hop Count) =Hi-Hf;
6) Use S to extract stored Hs (Hop count) from IP2HC mapping table;
7) If (Hc! = Hs)
8) The packet is spoofed;
9) Else
10) The Packet is legitimate;

This DoS prevention algorithm is used for detection of WSNs attack and dropping of spoofed packet. This algorithm is based on comparison of standard hop count stored in mapping table to the actual hop count obtained. After examining the hop count field in IP packet, hop count comparator perform comparison. If Hc! =Hs, it determines that the packet is spoofed, else the packet is legitimate and forwarded to energy watcher. [4]

VII. SIMULATION

The figure below displays the first page of the project. It displays the network and initializes all the nodes as well. It prompts the user to select the source node via which the packet is to be transmitted to the base station.

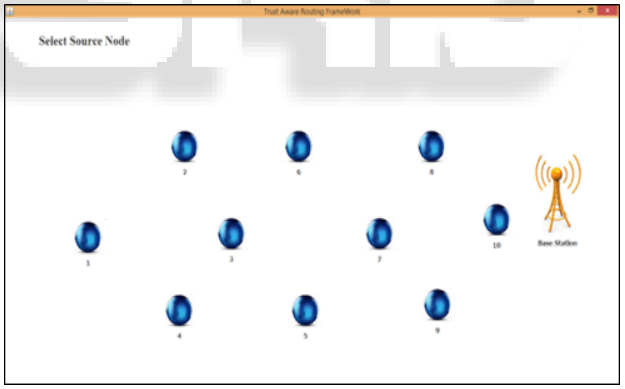

Fig. 3: Select Node

After selection of the source node a new form pops up to select the file that is to be transmitted.

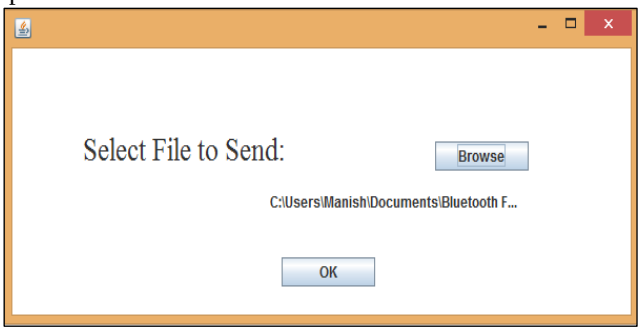

Fig. 4: New Popup Form

Later the transmission of packets takes place as displayed as in the below figure.

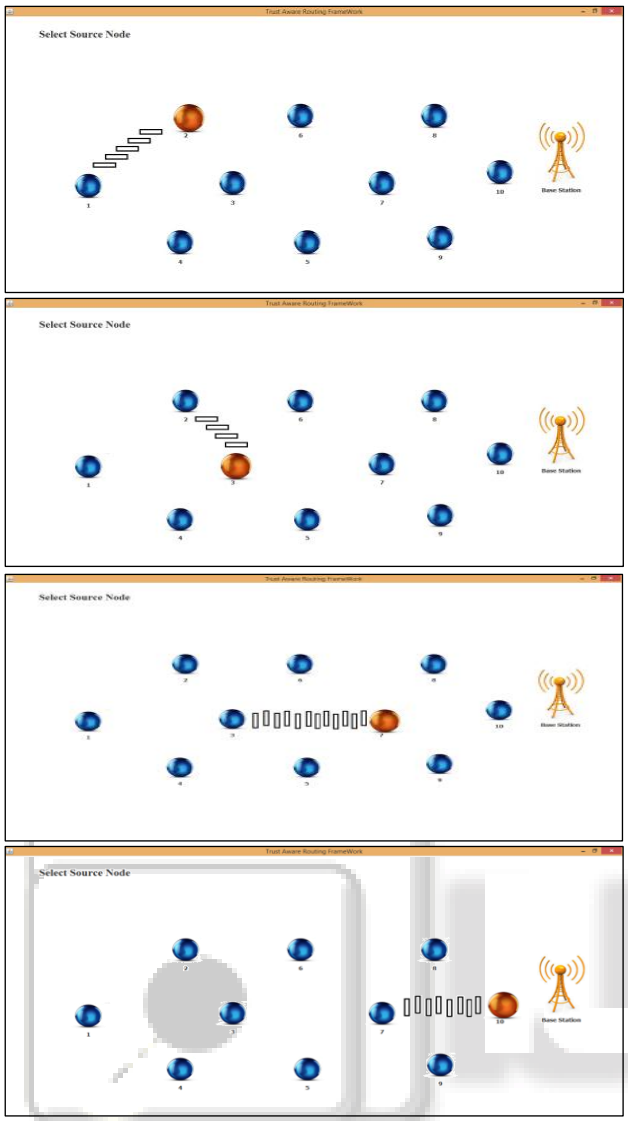

Fig. 5: transmission of packets

VIII. CONCLUSION

Proposed Trust Aware Routing Framework identifies various possible attacks on the wireless sensor networks. It also presents various defence mechanisms to counter the well-known attacks on the routing protocol of 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 this proposed system, an effort is made towards overcoming the deficiency of TARF against detection of and defence against DoS attacks.

REFERENCES

[1] Zhan Guoxing, Weisong Shi, and Julia Deng. "Design and implementation of TARF: a trust-aware routing framework for WSNs." Dependable and Secure Computing, IEEE Transactions on 9.2 (2012): 184-197.

[2] Rozner, Eric, et al. "SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks." Mobile Computing, IEEE Transactions on 8.12 (2009): 1622-1635.

[3] 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.

[4] 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.

[5] Sen, Jaydip. "Routing security issues in wireless sensor networks: attacks and defenses." arXiv preprint arXiv: 1101.2759 (2011).

[6] 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.

