International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 6, October 2014, PP 31-36
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Design and Implementation of TARF: A Trust–Aware Routing Framework WSN's

[1]M. Srikar Swamy [2]G.S. Uday Kiran

[1]P.G Student, Dept of CSE, BITS, Adoni, Kurnool
[2]Assoc Professor, Dept of CSE, BITS, Adoni, Kurnool

Abstract: *The multihop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks, and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multihop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. 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 RF-shielding network conditions. Further, we have implemented a low-overhead TARF module in TinyOS; as demonstrated, this implementation can be incorporated into existing routing protocols with the least effort. Based on TARF, we also demonstrated a proof-of-concept mobile target detection application that functions well against an antidetection mechanism.*

1. INTRODUCTION

Wireless sensor networks (WSNs) are ideal candidates for applications such as military surveillance and forest fire monitoring to report detected events of interest. A sensor node wirelessly sends messages to a base station via a multi-hop path with a narrow radio communication. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities. An attacker may tamper nodes physically, drop or misdirect messages in routes, create traffic collision with seemingly valid transmission, jam the communication channel by creating radio interference. The adversary is capable of launching harmful and hard-to-detect attacks against routing based on identity deception. As a harmful and easy-station. Such a fake base station could lure more than half the traffic, creating a "black hole".

The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. It greatly increases the chance of interaction between the honest nodes and the attackers, though mobility is introduced into WSNs for efficient data collection. A poor network connection causes much difficulty in distinguishing between an attacker and a honest node with transient failure. WSNs Without proper protection with existing routing protocols can be completely devastated under certain circumstances. Most existing routing protocols for WSNs either assume the honesty of nodes or focus on energy efficiency or attempt to exclude unauthorized participation by encrypting data and authenticating packets.

It is important to consider efficient energy use for battery powered sensor nodes and the robustness of routing under topological changes as well as common faults in a wild environment. The gossiping-based routing protocols offer certain protection against attackers by selecting random neighbors to forward packets, but at a price of considerable overhead in propagation time and energy use.

In addition, the cryptographic methods such as trust and reputation management have been employed in generic ad hoc networks and WSNs to secure routing protocols.

A system of trust and reputation management assigns each node a trust value according to its past performance in routing. The proposed trust and reputation management systems for generic ad hoc networks target only relatively powerful hardware platforms such as laptops and Smartphone's. Those systems cannot be applied to WSNs due to the excessive overhead for resource-constrained sensor nodes powered by batteries. Secure routing solutions based on trust and reputation management rarely address the identity deception through replaying routing information. The countermeasures proposed so far strongly depends on either tight time synchronization or known geographic information while their effectiveness against attacks exploiting the replay of routing information has not been examined yet. Based on the unique characteristics of resource-constrained WSNs the design of TARF centers on *trustworthiness* and to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity.

The malicious node then uses this forged identity to participate in the network routing to disrupting the network traffic. These routing protocols include the original headers that are replayed without any modification. After "stealing", that valid identity the malicious node is able to misdirect the network traffic. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques. *Sinkhole* attacks are another kind of attacks that can be launched after stealing a valid identity. A malicious node may claim itself to be a base station through replaying all the packets from a real base *energy efficiency*. The purpose of independent routing in the tarf 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.

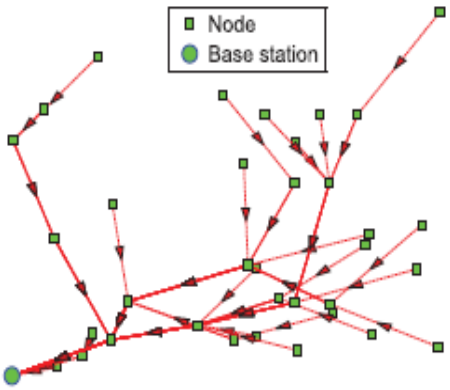

Fig. 1. Multihop routing for data collection of a WSN.

Most importantly, TARF proves resilient under various attacks exploiting the replay of routing information that is not achieved by previous security protocols. The effectiveness of TARF is verified through extensive evaluation with simulation and empirical experiments on large-scale WSNs. We have implemented a ready- to-use TARF module with low overhead that as demonstrated can be integrated into existing routing protocols with ease. The demonstration of a proof-of- concept mobile target detection program indicates the potential of TARF in WSN applications.

2. 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:

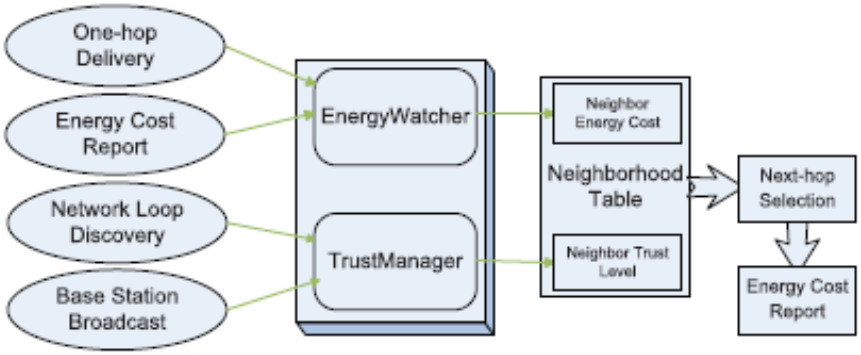

Fig.2. *Each node selects a next-hop node based on its neighborhood table, and broadcast its energy cost within its neighborhood. To maintain this neighborhood table, Energy Watcher and Trust Manager on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbors.*

(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 inMicroprocessor

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.

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 TARFenabled 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 neighbor 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 illustrate in the Fig 3

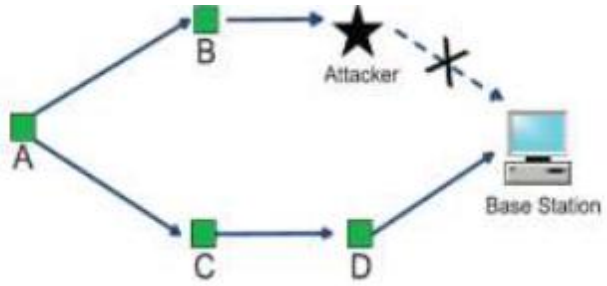

Fig 3. *A simple demonstration for Trust Manager*

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 routeselected, 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 retransmission may occur until the acknowledgement is received or the number of retransmissions 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 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 $EN \rightarrow b$, i.e., the average energy cost of successfully delivering a data packet from N to its neighbour b with one hop.

3. 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.

4. CONCLUSIONS

We have designed and implemented TARF, a robust trustaware routing framework for WSNs, to secure multihop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. Our main contributions are listed as follows:

1. Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information.

2. The resilience and scalability of TARF are proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves both static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

3. We have implemented a ready-to-use TinyOS module of TARF with low overhead; as demonstrated in the paper, this TARF module can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully functional protocols.

4. Finally, we demonstrate a proof-of-concept mobile target detection application that is built on top of TARF and is resilient in the presence of an anti detection mechanism that indicates the potential of TARF in WSN applications.

REFERENCES

[1]. G. Zhan, W. Shi, and J. Deng, "Tarf: A Trust-Aware Routing Framework for Wireless Sensor Networks," Proc. Seventh European Conf. Wireless Sensor Networks (EWSN '10), 2010.

[2]. F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004.

[3]. A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[4]. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

[5]. M. Jain and H. Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks," Proc. Int'l Conf. Advances in Computing, Control, and Telecomm. Technologies (ACT '09), pp. 555-558, 2009.

[6]. I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side," Proc. IEEE Int'l Conf. Wireless and Mobile Computing, Networking and Comm. (WIMOB '08), pp. 526-531, 2008.