International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12-13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

Review On-Implementation of Truthful Routing Path Generation in Wsns through Tarf

Ms Premakshi B.Dohe*, Mr. Rajesh Shukla**

*(Department of Software Engg., RGPV University, Bhopal(M.P)
Email: premadohe@gmail.com)
** (Department of Computer Science, RGPV University, Bhopal(M.P.)
Email: rkumardmh@gmail.com)

ABSTRACT
To face this problem, we propose a truthful routing protocol which adopts the routing principle to cope with the network dimensions, and relies on a distributed trust model for the detection and avoidance of malicious neighbors. 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 multi-hop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; Wireless sensor networks are vulnerable to a wide set of security attacks, including those targeting the routing protocol functionality. The multi-hop 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.

Keywords - Multi hop routing, RC6,Trusted Routing, TARF,Wireless sensor network.

I. Introduction

Wireless Sensor Networks (WSNs) offer efficient, low-cost solutions for a great variety of application domains including military fields, healthcare, homeland security, industry control, intelligent green aircrafts and traffic control in smart roads. Wireless sensor network is composed of a powerful base station and a set of low-end sensor nodes. Base station and sensor nodes have wireless capabilities and communicate through a wireless, multi-hop, ad-hoc network.[3]Wireless sensor networks (WSN) have emerged as an important new technology for instrumenting and observing the physical world.

Although networking and security technologies are in a mature stage, the limited sensor node resources in terms of memory space, processing power and energy availability, constrain the complexity of the security mechanisms that can be implemented, dictating the need for new protocol approaches design.

WIRELESS sensor networks (WSNs) are a capable scenario for sensing large areas at high spatial and positive resolution. However, the tiny size and low cost of the processing machines that makes them attractive for large deployment also causes the loss of low operational reliability[1].Wireless sensor networks (WSN) have emerged as an important new technology for instrumenting and observing the physical world. The basic building block of these networks is a tiny microprocessor integrated with one or more MEMS (micro-electromechanical system) sensors, actuators, and a wireless transceiver.[2] A WSN is usually collection of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the ability to gather data and route data back to a base station (BS). A sensor has four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit [5]. Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. Wireless sensor network contains large number of nodes and each node may be very close to each neighbor. Since WSN should use multihop techniques because it consume less power than single hop techniques.

Multihop techniques can also effectively overcome some of the signal propagation outcomes experienced in long-distance wireless communication [6]. WSN may also have additional application dependent components such as a location finding, system, power generator, and mobilizer (Fig. 1). Sensing units are usually composed of two sub units: sensors and analog-to-digital converters (ADCs). The ADCs

convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally related with a small storage unit, controls the procedures that make the sensor node collaborate with the other nodes. A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells).

CHARACTERSTICS OF WSN

The important characteristics of a WSN include

- Limited Power consumption for nodes using batteries or energy harvesting
- Ability to run with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of exploitation
- capacity to survive hard environmental conditions
- Easy to use
- Unattended operation
- Power consumption

As WSNs are lots of similar to traditional wireless ad hoc networks, important differences exist which greatly influence how security is achieved [4]. In [8], I. F. Akyildiz et al proposed the differences between sensor networks and ad hoc networks are:

1. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
2. Sensor nodes are densely deployed.
3. Sensor nodes are lying face down to failures due to harsh environments and energy constraints.
4. The topology of a sensor network changes very frequently due to failures or mobility.
5. Sensor nodes are limited in computation, memory, and power resources.
6. Sensor nodes may not have global identification.

Wireless sensor networks (WSNs) are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path. However, the multi-hop routing of WSNs often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference. Numerous security attacks have been presented in the literature ([6], [7]) with a significant subset targeting the routing process [8]. Once an adversary node manages to participate in the network, it can damage the routing process by simply dropping the packets it receives for forwarding, i.e. denying to sincerely cooperate in the routing procedure. Another easily implementable attack is packet modification. A taxonomy of routing attacks can be found in [9].

To defend against the majority of routing attacks, an approach borrowed from the human society has been proposed [10]: nodes monitor the behavior of their neighbors in order to evaluate their trustworthiness, regarding specific behaviour aspects called trust metrics.

Although a plethora of such models has been proposed and shown to efficiently mitigate routing attacks, trust models are themselves vulnerable to specific attacks [11]. The need to defend against these attacks further increases the complexity of the functionality that needs to be implemented on the sensor nodes for security purposes.

As a harmful and easy-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, thus disrupting the network traffic. Those routing packets, including their original headers are replayed without any modification. Even if this malicious node cannot directly overhear the valid node's wireless transmission, it can collude with Other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack. Since a node in a WSN usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. 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. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole". This same technique can be employed to conduct another strong form of attack - Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these

attacks. a poor network connection causes much difficulty in distinguishing between an attacker and a honest node with transient failure. Without proper protection, WSNs with existing routing protocols can be completely devastated under certain circumstances. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application. Unfortunately, most existing routing protocols for WSNs both 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. Admittedly, it is important to consider efficient energy use or battery powered sensor nodes and the robustness of routing under topological changes as well as common faults in a wild environment.However, it is also critical to incorporate security as one of the most important goals; meanwhile, even with perfect encryption and authentication, by replaying routing information, a malicious node can still participate in the network using another valid node's identity. 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 to the cryptographic methods, trust and reputation management has been employed in generic ad hoc networks and WSNs to secure routing protocols. Basically, a system of trust and reputation management assigns each node a trust value according to its past performance in routing. Then such trust values are used to help decide a secure and efficient route. However, the proposed trust and reputation management systems for generic ad hoc networks target only relatively powerful hardware platforms such as laptops and smart phones. Those systems cannot be applied to WSNs due to the excessive overhead for resource-constrained sensor nodes powered by batteries.

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:

1.1 Trusted AODV

The well-known AODV routing protocol has been extended by Xiaoqi Li et. al. to perform routing by taking into account trust metrics. A trust recommendation mechanism is first introduced and then the routing decision rules of AODV are modified to take into account trust. Of particular interest is that a set of policies is derived for a node to update its opinions towards others since, 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, Trust Update) are defined as well as the accompanying Route Table Extension, Routing Messages Extensions, Trusted Routing Discovery.

1.2 Trust-aware Dynamic Source Routing

To secure the Dynamic Source Routing (DSR) protocol, a mechanism involving the "watchdog" and "pathrater" modules has been designed and incorporated in the routing protocol.This scheme is applicable to routing protocols where the source defines the route to be followed by the packets. The mechanism basically consists of two components: Watchdog and Pathrater. The Watchdog is responsible for detecting selfish nodes that do not forward packets. To do so, each node in the network buffers every transmitted packet for a limited period. During this time, each node places its wireless interface into promiscuous mode in order to overhear whether the next node has forwarded the packet or not.

The Pathrater assigns different ratings to the nodes based upon the feedback that it receives from the Watchdog. These rating are then used to select routes consisting of nodes with the highest forwarding rate. The dynamic source routing (DSR) protocol that has been proposed to discover routes in wireless ad-hoc networks has been extended by Pirzada et. al to also take into account the trust levels (reputations) of the nodes. Exactly as happens in trusted AODV, it improves the achieved security although it cannot deal with all the possible attacks.

As far as WSNs are concerned, 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. At this point, to protect WSNs from the harmful attacks exploiting the replay of routing information, we have designed and implemented a robust trust-aware routing framework, TARF, to secure routing solutions in wireless sensor networks. Based on the unique characteristics of resource-constrained WSNs, the design of TARF centers on trustworthiness and energy efficiency. Though 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. Unlike other security measures, TARF requires neither tight time synchronization nor known geographic information. Most importantly, TARF proves resilient under various attacks exploiting the replay of routing information, which is not achieved by

previous security protocols. 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. The effectiveness of TARF is verified through extensive evaluation with simulation and empirical experiments on large-scale WSNs.

II. Considerations

In a data collection task, a sensor node sends its sampled data to a remote base station with the aid of other intermediate nodes, as shown in Figure 1. Though there could be more than one base station, our routing approach is not affected by the number of base stations; to simplify our discussion, we assume that there is only one base station. An adversary may forge the identity of any legal node through replaying that node's outgoing routing packets and spoofing the acknowledgement packets,even remotely through a wormhole.

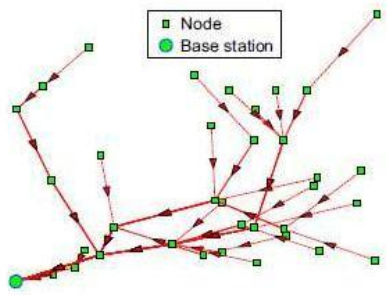

Fig.1. Multi-hop routing for data collection of a WSN Nonetheless, our approach can still be applied to cluster based WSNs with static clusters, where data are aggregated by clusters before being relayed. Cluster-based WSNs allows for the great savings of energy and bandwidth through aggregating data from children nodes and performing routing and transmission for children nodes. In a cluster-based WSN, the cluster headers themselves form a sub-network; after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a sub-network consisting of the cluster headers. Our framework can then be applied to this sub-network to achieve secure routing for cluster based WSNs. TARF may run on cluster headers only and the cluster headers communicate with their children nodes directly since a static cluster has known relationship between a cluster header and its children nodes, though any link-level security features may be further employed. Finally, we assume a data packet has at least the following fields: the sender id, the sender sequence number, the next-hop node id (the receiver in this one hop transmission), the source id (the node that initiates the data), and the source's sequence number. We insist that the source node's information should be included for the following reasons because that allows the base station to track whether a data packet is delivered. It would cause too much overhead to transmit all the one hop information to the base station. Also, we assume the routing packet is sequenced.

III. Goals

TARF mainly guards a WSN against the attacks misdirecting the multi-hop routing, especially those based on identity theft through replaying the routing information. This paper does not address the denial-of-service (DoS) attacks, where an attacker intends to damage the network by exhausting its resource. For instance, we do not address the DoS attack of congesting the network by replaying numerous packets or physically jamming the network. TARF aims to achieve the following desirable properties:

3.1High Throughput

Throughput is defined as the ratio of the number of all data packets delivered to the base station to the number of all sampled data packets. Through put reflects how efficiently the network is collecting and delivering data. Here we regard high throughput as one of our most important goals.

3.2 Energy Efficiency

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

3.3 Scalability & Adaptability

TARF should work well with WSNs of large magnitude under highly dynamic contexts. We will evaluate the scalability and adaptability of TARF through experiments with large-scale WSNs and under mobile and hash network conditions.

IV. Design Of Tarf

TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes.

It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TARF is also energy efficient, highly scalable, and well adaptable. Before introducing the detailed design, we first introduce several necessary notions here.

4.1 Neighbor

For a node N, a neighbor (neighboring node) of N is a node that is reachable from N with one-hop wireless transmission.

4.2 Trust level

For a node N, the trust level of a neighbor is a decimal number in [0, 1], representing N's opinion of that neighbor's level of trustworthiness. Specifically, the trust level of the neighbor is N's estimation of the probability that this neighbor correctly delivers data received to the base station.

4.3 Energy cost

For a node N, the energy cost of a neighbor is the average energy cost to successfully deliver a unit sized data packet with this neighbor as its next-hop node, from N to the base station.

4.4 OVERVIEW

For a TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the trustworthiness and the energy efficiency. Once the data packet is forwarded to that next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. In TARF, in addition to data packet transmission, there are 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 message needs acknowledgement. A broadcast message from the base station is flooded to the whole network. The freshness of a broadcast message is checked through its field of source sequence number. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbors once. Any node receiving such an energy cost report message will not forward it. For each node N in a WSN, to maintain such a neighborhood table with trust level values and energy cost values for certain known neighbors, two components, Energy Watcher and TrustManager, run on the node (Figure 2).

4.4.1 Energy Watcher is Responsible for Recording the Energy Cost for each known neighbor, based on N's observation of one-hop transmission to reach its neighbors and the energy cost report from those neighbors. A compromised node may falsely report an extremely low energy cost to lure its neighbors into selecting this compromised node as their next-hop node; however, these TARF-enabled neighbors eventually abandon that compromised next hop node based on its low trustworthiness as tracked by TrustManager. TrustManager is responsible for tracking trust level values of neighbors based on network loop discovery and broadcast messages from the base station about data delivery. Once N is able to decide its next hop neighbor according to its neighborhood table, it sends out its energy report message: it broadcasts to all its neighbors its energy cost to deliver a packet from the node to the base station.

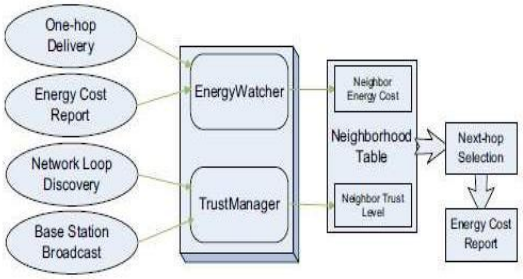

Fig.2 Each node select a next-hop node based on its neighborhood table,and broadcast its energy cost within its neighborhood.

4.4.2 Implementation And Empirical Evaluation

The routing and trust overhead introduced by ATSR includes the Beacon (broadcast) message which is used by each node to periodically announce its location coordinates, node id and remaining energy, the reputation request (multicast) message used to periodically request indirect trust information and the reputation response (unicast) message which is used to provide indirect information as a reply to a reputation request message. Starting from the direct trust, each neighbor is evaluated based on a set of trust metrics which include:

4.4.2.1 Packet forwarding

To detect nodes that deny to or selectively forward packets, acting in a selfish (malicious or not) manner, each time a source node sends a packet to a neighbor for further forwarding, it enters the promiscuous mode and overhears the wireless medium to check whether the packet was actually forwarded by the selected neighbor.

4.4.2.2 Network layer Acknowledgements (ACK)

To detect the successful end-to-end forwarding of the messages (and detect colluding adversaries), we suggest that each source node waits for a network-

layer ACK per transmitted message to check whether the message has successfully reached a higher layer node (i.e. the base station). It is stressed that this check is performed only
for trust evaluation purposes and does not necessarily trigger any message retransmission.

4.4.2.3 Packet precision

Each time a source node transmits a packet for forwarding and then overhears the wireless medium to ensure that the packet was forwarded, it additionally processes it to check the packet's integrity, i.e. that no unexpected modification has occurred.

4.4.2.4 Authentication

The trust management module receives information from other (higher layer) blocks related to the trustworthiness of the neighbors. For example, in case a node may choose among neighbors supporting different authentication mechanisms, the one with better security features should be preferred. Although this is not an event or behaviour aspect monitored by the source node, it is listed here as an input to the trust evaluation system.

4.4.2.5 Reputation Response

To check the sincere execution of the reputation exchange protocol, the node that requests reputation information, calculates for each neighbor the number of received reputation responses divided by the number of times this neighbor was asked for reputation information. This way, nodes that do not cooperate in the execution of the reputation protocol (acting in a selfish manner) are assigned lower trust values and are avoided for forwarding co-operations as a penalty.

4.4.2.6 Reputation Validation

To protect against wrong (either bad or good) reputations being spread around (called hereafter bad-mouthing attack) and conflicting behaviour attacks [11] (i.e. a malicious node behaves differently towards different neighbors in different timespans), each time a reputation response message is received, the received reputations are validated. Each
time node A receives a reputation response message from node C regarding node B, it compares it with the trust value node A has calculated for node B (if node A is confident about the direct trust value) and with the reputations provided by other neighbors. If the difference between the received value and the others exceeds a certain threshold, then the node that provided this value is considered malicious and the reputation is considered wrong; otherwise it is a "correct reputation".

4.4.2.7 Remaining Energy

Although the energy level of each neighbor is not a pure trust metric, taking into account the remaining energy level, apart from extending the network lifetime, contributes towards load balancing (partially defending against the traffic analysis attack). In our novel routing protocol, the remaining energy travels piggy-backed in the Beacon message used to indicate the node availability and position.

V. Conclusions

We have designed and implemented TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of 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. 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. The resilience and scalability of TARF is proved through both extensive simulation and empirical evaluation with large-scaleWSNs; the evaluation involves static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, "*TARF: A trust-aware networks*," in Proceeding of the 7th *European Conference on Wireless Sensor Networks (EWSN'10), 2010.*

[2] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. *Morgan Kaufmann Publishers, 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*," in Proceedings of the 1st *IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*

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

[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, "*Launching a sinkhole attack in wireless sensor networks; the intruder side*," in Proceedings of *IEEE International Conference on Wireless and Mobile Computing, Network.*

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attackin sensor networks: Analysis and

defenses," in *Proc. of the 3rd International Conference on Information Processing in Sensor Networks(IPSN'04), Apr. 2004*.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysisof mobile agent-based wireless sensor network," in *Proceedingsof the 8th International Conference on Reliability, Maintainability andSafety (ICRMS 2009), 20-24 2009, pp. 16 –19.*

[9] L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middlewarefor wireless sensor networks data fusion," in *Proceedingsof Instrumentation and Measurement Technology Conference (I2MTC'09), 5-7 2009, pp. 378 –383*.

[10] W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based movingtarget methods in wireless sensor networks," in *IEEE InternationalSymposium on Communications and Information Technology (ISCIT2005)*, vol. 1, 12-14 2005, pp. 22 – 26.

[11] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "Amobile agent based leach in wireless sensor networks," in *Proceed-ings of the 10th International Conference on Advanced CommunicationTechnology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 – 78.

[12] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensornetworks: a survey," *Wireless Communications*, vol. 11, no. 6, pp.6–28, Dec. 2004.