International Journal
of Computer Sciences

IMPLEMENTATION OF ENERGY EFFICIENT AND TRUST AWARE ROUTING FOR WSNs

S. Selva Kumar

Assistant Professor
Department of computer science and engineering
SRM Univeristy
Tamil Nadu, India-603203

Gandharva Reddy Puli

Department of Computer Science and Engineering
SRM Univeristy
Tamil Nadu-603203.
Email- gansmile1424@gmail.com

Abstract:

To compute the trusted aware routing in wireless sensor networks and avoiding the attackers in the networking. For providing security from attackers in the network we study 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. 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. 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. Further, we have implemented a low-overhead TARF module and demonstrated this implementation can be incorporated into existing routing protocols with the least effort.

1. INTRODUCTION

TARF, a robust trust-aware routing framework for WSNs, have been designed and implemented, 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-scale WSNs; the evaluation involves static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

A ready-to-use Tiny OS module of TARF with low overhead have been used till now. However this TARF module can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully-functional protocols. Finally 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 is proposed that indicates the potential of TARF in WSN applications. 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 sensor 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.

This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception, the

adversary is capable of launching harmful and hard-to-detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks and Sybil attacks.

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. 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. Though mobility is introduced into WSNs for efficient data collection and various applications, it greatly increases the chance of interaction between the honest nodes and the attackers.

Additionally, 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. 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.

2. RELATED WORKS

Zhan. G, Shi.W, Deng.J [1] have investigated that what assumptions are necessary to gather information about the local network topology when adversarial nodes are present and capable of lying about their identity or neighbors in the network. Many sensor network protocols utilize the existence of disjoint paths (e.g., perfectly secure message transmission or multi-path key establishment), but do not address how a node actually determines these paths in the presence of an adversary. These assumptions are practical, and realizable through existing tools such as combinatorial key pre-distribution, fingerprinting, and localization. The protocols ensure that, except with small probability, if node accepts a path through the network as valid, then each node along that path must be telling the truth about its identity and nodes it can communicate with, so long as a majority of honest nodes are present in the network at each point decisions are made.

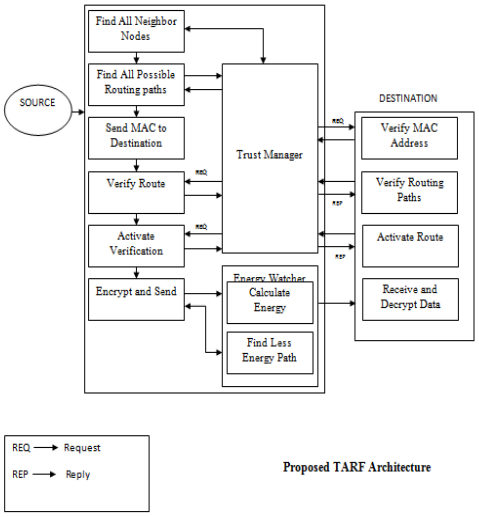
Karlof.C, Wagner.D [2] proposed that trusted mechanism is evaluated for the potential application on resource constraint devices by quantifying their power consumption on selected major processes. Secure communication mechanisms in Wireless Sensor Networks (WSNs) have been widely deployed to ensure confidentiality, authenticity and integrity of the nodes and data. Recently many WSNs applications rely on trusted communication to ensure large user acceptance. Indeed, the trusted relationship thus far can only be achieved through Trust Management System (TMS) or by adding external security chip on the WSN platform. In this study an alternative mechanism is proposed to accomplish trusted communication between sensors based on the principles defined by Trusted Computing Group (TCG). The results of other related study have also been analyzed to validate and support our findings. The result proved the proposed scheme can establish trust in WSN with less computation and communication and most importantly eliminating the need for neighboring evaluation for TMS or relying on external security chip.

Jain.M, Kandwal.H [3] explained wireless communication faces several security risks. An attacker can easily inject bogus packets, impersonating another sender. This attack is referred to as a spoofing attack. An attacker can also easily eavesdrop on communication record packets, and replay the (potentially altered) packets. In this paper, we are concerned of a particularly severe security attack that affects the ad hoc networks routing protocols, it is called the wormhole attack. In the first phase, these malicious nodes, called wormhole nodes, try to lure legitimate nodes to send data to other nodes via them. In the second phase, wormhole nodes could exploit the data in variety of ways.

Bai.L, Ferrese.F, Ploskina.K and Biswas.S [4] describes a reliability model which can be used to analyze the performance and power consumption in resource constrained, data rate scarce, mobile agent-based wireless sensor network (WSN) systems. The primary model is referred to as a generalize access structure congestion (GGC) system which is an extended model from a circular sequential k-out-of-n congestion (CSknC). There are many other reliability models which can be used to study WSN systems, but they are not suitable to analyze and address mobile agent-based multisensory WSN systems. By employing mobile agent technologies, the systems can make accurate decisions quickly and reduce data rate and data redundancy problems. An important research problem is to determine how to maintain efficient duty cycle by using multiple types of sensors without centralized architecture and with mobile agent technologies.

3. PROPOSED WORK

In proposed System, focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception the adversary is capable of launching harmful and hard to detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks, and Sybil attacks.



Proposed TARF Architecture

3.1 Routing the Network and transfer file

TARF, as with many other routing protocols, runs as a periodic service. The length of that period determines how frequently routing information is exchanged and updated. At the beginning of each period, the base station broadcasts a message about data delivery during last period to the whole network consisting of a few contiguous packets. Whenever a node receives such a broadcast message from the base station, it knows that the most recent period has ended and a new period has just started. No tight time synchronization is required for a node to keep track of the beginning or ending of a period. During each period, the *EnergyWatcher* on a node monitors energy consumption of one-hop transmission to its neighbors and processes energy cost reports from those neighbors to maintain energy cost entries in its neighborhood table; its *TrustManager* also keeps track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its neighborhood table. To maintain the stability of its routing path, a node may retain the same next-hop node until the next fresh broadcast message from the base station

occurs. Meanwhile, to reduce traffic, its energy cost report could be configured to not occur again until the next fresh broadcast message from the base station. If a node does not change its next-hop node selection until the next broadcast message from the base station, that guarantees all paths to be loop-free, as can be deducted from the procedure of next-hop node selection. However, as noted in our experiments, that would lead to slow improvement in routing paths. Therefore, we allow a node to change its next-hop selection in a period when its current next-hop node performs the task of receiving and delivering data poorly.

3.1.1 *Structure and Exchange of Routing Information*

A broadcast message from the base station fits into at most a fixed small number of packets. Such a message consists of some pairs of <node id of a source node, an undelivered sequence interval [a, b] with a significant length>, <node id of a source node, minimal sequence number received in last period, maximum sequence number received in last period>, as well as several node id intervals of those without any delivery record in last period. To reduce overhead to an acceptable amount, our implementation selects only a limited number of such pairs to broadcast. Roughly, the effectiveness can be explained as follows: the fact that an attacker attracts a great deal of traffic from many nodes often gets revealed by at least several of those nodes being deceived with a high likelihood. The undelivered sequence interval [a,b] is explained as follows: the base station searches the source sequence numbers received in last period, identifies which source sequence numbers for the source node with this id are missing, and chooses certain significant interval [a, b] of missing source sequence numbers as an undelivered sequence interval. For example, the base station may have all the source sequence numbers for the source node 2 as {109, 110, 111, 150, 151} in last period. Then [112, 149] is an undelivered sequence interval; [109, 151] is also recorded as the sequence boundary of delivered packets. Since the base station is usually connected to a powerful platform such as a desktop, a program can be developed on that powerful platform to assist in recording all the source sequence numbers and finding undelivered sequence intervals. Accordingly, each node in the network stores a table of <node id of a source node, a forwarded sequence interval [a, b] with a significant length> about last period. The data packets with the source node and the sequence numbers falling in this forwarded sequence interval [a, b] have already been forwarded by this node.

When the node receives a broadcast message about data delivery, its *TrustManager* will be able to identify which data packets forwarded by this node are not delivered to the base station. Considering the overhead to store such a table, old entries will be deleted once the table is full. Once a fresh broadcast message from the base stationis received, a node immediately invalidates all the existing energy cost entries: it is ready to receive a new energy report from its neighbors and choose its new next-hop node afterwards. Also, it is going to select a node either after a timeout is reached or after it has received an energy cost report from some highly trusted candidates with acceptable energy cost. A node immediately broadcasts its energy cost to its neighbors only after it has selected a new next-hop node. That energy cost is computed by its *EnergyWatcher*.

3.1.2 Route Selection

Each node N relies on its neighborhood table to select an optimal route, considering both energy consumption and reliability. TARF makes good efforts in excluding those nodes that misdirect traffic by exploiting the replay of routing information. For a node N to select a route for delivering data to the base station, N will select an optimal next-hop node from its neighbors based on trust level and energy cost and forward the data to the chosen next-hop node immediately. The neighbors with trust levels below a certain threshold will be excluded from being considered as candidates. Among the remaining known neighbors, N will select its next-hop node through evaluating each neighbor b based on a trade-off between TNb and ENb/TNb, with ENb and TNb being b's energy cost and trust level value in the neighborhood table respectively.

Basically, ENb reflects the energy cost of delivering a packet to the base station from N assuming that all the nodes in the route are honest; 1/TNb approximately reflects the number of the needed attempts to send a packet from N to the base station via multiple hops before such an attempt succeeds, considering the trust level of b. Thus, ENb TNb combines the trustworthiness and energy cost. However, the metric ENb /TNb suffers from the fact that andversary may falsely reports extremely low energy cost to attract traffic and thus resulting in a low value of ENb /TNb even with a low TNb. Therefore, TARF prefers nodes with significantly higher trust values; this preference of trustworthiness effectively protects the network
from an adversary who forges the identity of an attractive node such as a base station. For deciding the next-hop node, a specific trade-off between TNb and ENb, TNb

3.2 Energy Watcher

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 E_{Nb}. Suppose N decides that A should be its next-hop node after comparing energy cost and trust level. Then N's energy cost is $E_N = E_{NA}$. Denote $E_{N!b}$ as the average energy cost of successfully delivering a data packet from N to its neighbor 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:

$$ENb = EN!b + Eb$$

Since each known neighbor 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 neighbor b with one hop. For that, assuming that the endings (being acknowledged or not) of onehop transmissions from N to b are independent with the same probability psucc of being acknowledged. Denote E_{unit} as the energy cost for node N to send a unit-sized data packet once regardless of whether it is received or not. The two parameters $w_{degrade}$ and $w_{upgrade}$ allow flexible application requirements. $w_{degrade}$ and $w_{upgrade}$ represent the extent to which upgraded and degraded performance are rewarded and penalized, respectively. If any fault and compromise is very likely to be associated with a high risk, $w_{degrade}$ should be assigned a relatively high value to penalize fault and compromise relatively heavily; if a few positive transactions can't constitute evidence of good connectivity which requires many more positive transactions, then $w_{upgrade}$ should be assigned a relatively low value.

3.3 Trust Manager

A node N's *TrustManager* decides the trust level of each neighbor based on the following events: discovery of network loops, and broadcast from the base station about data delivery. For each neighbor b of N, TNb denotes the trust level of b in N's eighborhood table. At the beginning, each neighbor is given a neutral trust level 0.5. After any of those events occurs, the relevant neighbors' trust levels are updated.

Note that many existing routing protocols have their own mechanisms to detect routing loops and to react accordingly. In that case, when integrating TARF into those protocols with anti-loop mechanisms, *TrustManager* may solely depend on the broadcast from the base station to decide the trust level; we adopted such a policy when implementing TARF later. If anti-loop mechanisms are both enforced in the TARF component and the routing protocol that integrates TARF, then the resulting hybrid protocol may overly react towards the discovery of loops. Though sophisticated loop-discovery methods exist in the currently developed protocols, they often rely on the comparison of specific routing cost to reject routes likely leading to loops. To minimize the effort to integrate TARF and the existing protocol and to reduce the overhead, when an existing routing protocol does not provide any antiloop mechanism, we adopt the following mechanism to detect routing loops. To detect loops, the *TrustManager* on N reuses the table of <node id of a source node, a forwarded sequence interval [a, b] with a significant length>. If N finds that a received data packet is already in that record table, not only will the packet be discarded, but the TrustManager on N also degrades its next-hop node's trust level. If that next-hop node is b, then Told Nb is the latest trust level value of b. We use a binary variable Loop to record the result of loop discovery: 0 if a loop is received; 1 otherwise.

3.4 Sinkhole and wormhole attacks

This prevents the base station from obtaining complete and correct sensing data Particularly severe for wireless sensor networks. Some secure or geographic based routing protocols resist to the sinkhole attacks in certain level Many current routing protocols in sensor networks are susceptible to the sinkhole attack. Set of sensor nodes continuously monitor their surroundings forward the sensing data to a sink node, or base station. Many-to-one Communication vulnerable to the sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information alters the data passing through it or performs selective forwarding.

4. CONCLUSION

TARF has been designed and implemented, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmfulattackers 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. 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 both static and mobile settings, hostile network conditions, as well as strong attacks such as *wormhole* attacks and *Sybil* attacks. 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. 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 inWSN applications.

5. REFERENCES

[1] Chris Karlof and David 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.*

[2] Guoxing Zhan, Weisong Shi, and Julia Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," *in Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10), 2010*

[3] Li Bai, Frank Ferrese, Kathryn Ploskina, and Saroj Biswas, "Performance analysis of mobile agent-based wireless sensor network," *in Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009), 20-24 2009, pp. 16 –19.*

[4] Mohit Jain and Himanshu 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.*

BIOGRAPHY

Gandharva Reddy Puli, Department of Computer Science and Engineering, SRM Univeristy, Tamil Nadu-603203. Email: gansmile1424@gmail.com

S. Selva Kumar, received M.Tech Degree from SRM University, Chennai, he published several papers National and International and attended several Conferences. He is working as Assistant Professor, Department of computer science and engineering, SRM Univeristy, Tamil Nadu, India-603203