Volume 1 , Issue 6, PP: 62 - 69 , SEPTEMBER 2014.

AN IMPREGNABLE MULTI-HOP ROUTING IN WI-FI SENSOR NETWORKS

MANDE JAKRAYYA 1*, K.RAMALINGA REDDY 2*

1. *II.M.Tech , Dept of CSE, AM Reddy Memorial College of Engineering & Technology, Petlurivaripalem.*
2. *Asst Prof, Dept. of CSE, AM Reddy Memorial College of Engineering & Technology, Petlurivaripalem.*

Abstract

The multi-hop routing in wireless sensor networks offers little fortification against identity trickery through replaying routing information. An opponent can exploit this defect to launch various harmful or even overwhelming attacks against the routing protocols, including sinkhole attacks, wormhole attacks and Sybil attacks. The situation is further provoked by portable and ruthless 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, a method has been designed and implemented a robust trust-aware routing framework for self-motivated WSNs. Without tight time synchronization or known geographic information, it provides dependable and energy-efficient route. The flexibility of trusted routing is verified through extensive evaluation with both replication and pragmatic experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. This paper evaluates the proposed TARP protocols on two important attributes, the *battery power* and the *software configuration*. This protocol also is able to improve security and at the same time reduce the total routing traffic sent and received in the network by directing the traffic based on the requested sender attributes.

Keywords: TARF, WSN's, Ad Hoc, Power, Cryptography.

1. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration [1]. The absence of any central coordination or base station makes the routing complex when compared with regular cellular networks. Several protocols have been introduced for Ad Hoc routing. The issues related to the design of the ad hoc routing protocols are inherently related to the ad hoc application. Routing protocols are designed for purposes such as quality of service provisioning, energy management and security. A noteworthy on-demand protocol called Dynamic Source Routing (DSR) protocol [2]. DSR was designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. The problem of routing was divided into two areas - route

discovery and route maintenance. In order for one host to communicate with another, it must initially discover a suitable route to use in sending packets to that destination. As long as conditions remain unchanged, this route should be maintained as long as it is needed. An attacker may interfere nodes physically, create traffic collision with apparently valid broadcast, drop or misdirect post in routes, or pack the communication channel by creating broadcasting intrusion. As a harmful and easy-to-implement type of hit, a spiteful node simply replays all the outgoing routing packets from a valid node to copy the latter node's character; 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. 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. 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. Even form a transmission loop through which packets are passed among a few malicious nodes infinitely. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. 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. Those systems cannot be applied to WSNs due to the excessive overhead for resource-constrained sensor nodes powered by batteries. As far as WSNs are concerned, secure routing solutions based on trust and reputation management rarely address the identity deception through replaying routing information . 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. 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. TRUST AWARE ROUTING PROTOCOL

The main objectives of the proposed protocol are: (a) implement security that is intrinsically built into the map-reading procedure, (b) deliver communication that are received with best available level of self-confidence, (c) allow users and applications to set their

required level of defense, (d) achieve effectiveness in routing that is improved by restrictive control message interactions, (e) optimize resource usage, (f) achieve elegant network routine deprivation, and (g) extend a procedure suite that adapts to changes in the atmosphere, such as the network topology, the power-level of nodes, etc.The security parameters considered in computing the trust-level of a node in a given route include: *software design*, *hardware design*, *battery power*, *credit record*, *publicity* and *executive pecking order*. Each node validates the trust level of its neighbors based on the above parameters and includes it in computing the next hop node in the overall shortest route estimation. Due to page restrictions, this paper will focus on the implementation and evaluation of the battery power and the software configuration attributes.

1. In wireless networks, the battery power with which nodes operate is a limited resource. Each node uses its power to not only send and receive, it also behaves as a router by forwarding routing messages and updates. The cryptographic techniques that provide security is computationally intensive, which further increase the power consumption of a node.
2. Software design: The software design includes the encryption ability of a node. To satisfy SAR (Secrecy, Accessibility and Reliability), different cryptographic mechanisms have been proposed. Some are based on symmetric encryption and others on asymmetric encryption. Each node is given either a shared secret key or a public/private key pair depending on the type of cryptographic mechanism. Strong encryption is often discerned by the key length used by the algorithm. In general, a node with a stronger encryption algorithm has a higher trust level than a node with a weaker encryption algorithm.

3. DESIGN 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.

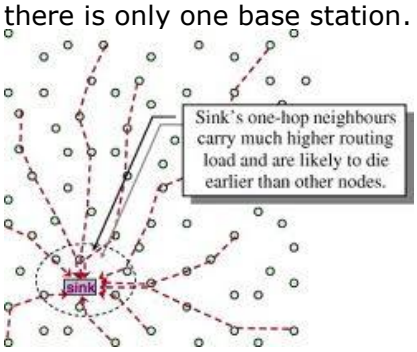

Fig 1: Multi-hop routing for data collection of a WSN

Trusted Protocol secures the multi-hop routing in WSNs against intruders exploiting the replay of routing information by evaluating the trustworthiness of neighboring nodes. TARF is also energy-efficient, highly scalable, and well adaptable.

3.1 Overview

Trusted Routing integrates trustworthiness and energy efficiency in making routing decisions. For a node *N* to route a data packet to the base station, *N* only needs to decide to which A Trust-Aware Routing Framework for Wireless Sensor Networks neighboring node it should forward the data packet. That chosen neighbor is *N*'s next hop node. 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. To choose its next-hop node, N considers both the trustworthiness and the energy efficiency of its neighbors. For that, *N* maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. It is sometimes necessary to delete some neighbors' entries to keep the table size acceptable. Maintaining a neighborhood table with acceptable overhead proved possible in [17]; the same technique can be used by 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 undelivered data packets and energy cost report messages from each node. A broadcast message from the base station is broadcast to the whole network; each node receiving a fresh broadcast message from the base station will broadcast it to all its neighbors once. The freshness of a broadcast message is ensured by 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. Additionally, 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*

Route Selection: Now, we introduce how TARF decides routes in a WSN. 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 forwards the data to the chosen next-hop node immediately.

Among the remaining known neighbors, *N* will select as its next-hop node a neighbor *b* with the minimal value of *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, comparing the values of *ENb TNb* among *N*'s neighbors identifies a candidate with a minimal combined cost of energy and trustworthiness. The remaining delivery task is fully delegated to that selected next-hop neighbor, and *N* is totally unaware of what routing decision its chosen neighbor is going to make.

4 Performances and Experimental Estimation

We have implemented a protocol based on TARF in TinyOS 1.x, which currently runs on mica2 motes. Both the authentication and encryption of packets reuse the implementation of TinySec [4]: TinySec uses a CBC mode encryption scheme with Skipjack as the block cipher and an authentication scheme based on a four-byte message authentication code (MAC) computed by the CBC-MAC construction procedure. The MAC field is computed over the whole message including all the headers; it also serves as the CRC field of the packet. In a routing packet, the next-hop id is replaced by a neighborhood broadcast address or a network broadcast address to indicate that it is a neighborhood or whole network broadcast. The acknowledgement of data packets is enabled. The implementation uses an integer in [0*,* 100] to represent trust level; the update of energy cost and trust level values is also implemented using integer arithmetic.

This implemented TARF protocol requires moderate program storage and memory usage. For comparison, we list the ROM size and RAM size requirement for this protocol and two other protocols on mica nodes in Table 1.

Table 1. Size of protocol components implemented

Protocol	Authentication Encryption	ROM (bytes)	RAM (bytes)
TARF	TinySec	20912	1464
Route	TinySec	20696	1048
MintRoute	TinySec	22554	1990

The experiment (Figure 4(a)), all nodes on the three floors was supposed to deliver data to node the base station;

node fake base station replayed all the routing packets from the base station. By counting the data packets received at the real base station, Trust Routing had roughly a 59% higher *throughput* than *CTP*. In another experiment (Figure 4(b)), only the nodes on the first floor i.e., 56 nodes totally sent data to node the base station, and fake base station replayed the routing packets from the base station. As a result, this routing had approximately a 41% higher *throughput* than *CTP*. We also recorded the number of redundant data packets received by the base station. Though both CTP and TARF suppress redundant packets, a packet might be received more than once by the base station because an acknowledgment is lost when the route changes

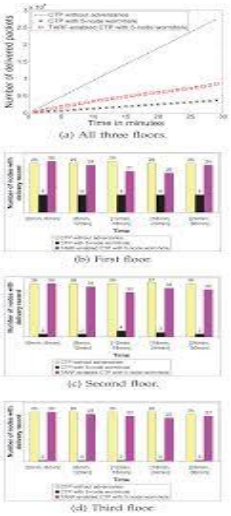

Fig 2: Empirical comparison of CTP and TARF-enabled CTP on Matlab: (a) number of all delivered data packets since the beginning; number of nodes on (b) the first floor, (c) the second floor and (d) the third floor that delivered at least one data packet in sub-periods.

5. CONCLUSIONS

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 was implemented successfully. Trusted routing focused on trustworthiness and energy efficiency, which are very important to the endurance of a WSN in an aggressive environment. With the idea of trust management, it enabled a node to keep track of the dependability of its neighbors and thus to select a reliable route. The results of implementing the software configuration and the battery power have been presented. The routing traffic is directly related to the number of nodes that meet the sender's requirements. To combine the effects of different trust attributes into one trust metric and evaluate the performance of TARP based on the collective metric. We demonstrated 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] Yih-Chun Hu and D. B. Johonson, "Securing Quality-of-Service Route

Discovery in On-Demand Routing for Ad Hoc Networks," *Proceedings of ACM SASN '04*, October 20, 2004.

[2] W. Lou and W. Liu, and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," *Proceedings of IEEE INFOCOM 2004*, 2004

[3] Boukerche, A., El-Khatib, K., Xu, L., Korba, L.: A novel solution for achieving anonymity in wireless ad hoc networks. In: Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, pp. 30–38 (2004)

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

[5] Karlof, C., Sastry, N., Wagner, D.: Tinysec: A link layer security architecture for wireless sensor networks. In: Proc. of ACM SenSys 2004 (November 2004)

[6] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, 1995.

[7] Matlab, http://www.mathworks.com

[8] Motelab, http://motelab.eecs.harvard.edu.

[9] D. B. Johnson and D. A. Maltz, "Dynamic Sources Routing in ad Hoc Wireless Networks," *Mobile Computing*, 1996

[10] Wood, A., Stankovic, J.: Denial of service in sensor networks. Computer 35(10), 54–62 (2002)

[11] S. Buchegger and Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes—Fairness In Dynamic Ad-hoc Networks,"*Proceedings*

[12] *of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2002

[13] Al-Karaki, J., Kamal, A.: Routing techniques in wireless sensor networks: a survey. IEEEWireless Communications 11(6), 6–28 (2004)

.Zhan, G., Shi, W., Deng, J.: Poster abstract: Sensortrust - a resilient trust model for wsns. In: SenSys 2009: Proceedings of the 7th International Conference on Embedded Networked Sensor Systems (2009)

[14] G. Zhan, W. Shi, and J. 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.

M Jakrayya , et al , International Journal of Computers Electrical and Advanced Communication Engineering [IJCEACE]™

Volume 1 , Issue 6, PP: 62 - 69 , SEPTEMBER 2014.