M.Vinoth *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 2, February- 2014, pg. 30-37 **ISSN: 2321-8363**

Efficient Routing from Multiple Sources to Multiple sinks in Wireless Sensor Networks

Mr. M.Vinoth[1], Ms. N.Radhika[2]

[1]PG Student, [2]Assistant Professor, Department of Computer Science and Engineering,

PRIST University, Trichy District, India

[1] vino.fb@gmail.com

ABSTRACT

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. 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 Tiny OS; 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.

Index Terms—Wireless sensor networks, routing protocols, security

I.INTRODUCTION

WIRELESSSENSOR networks (WSNs) [2] 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 multihop path. However, the multihop 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 [6]. 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 [7]: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. 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. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application.

II.RELATED WORK

2.1 DESIGN CONSIDERATIONS

Before elaborating the detailed design of TARF, we would like to clarify a few design considerations first, including certain assumptions in Section 2.1 and the goals in Section 2.3.

2.1.1 Assumptions

We target secure routing for data collection tasks, which are one of the most fundamental functions of WSNs. In a data collection task, a sensor node sends its sampled data to a remote base station with the aid of other intermediate nodes, as shown in Fig. 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 acknowledgment packets, even remotely through a wormhole. Additionally, to merely simplify the introduction of TARF, we assume no data aggregation is involved. Nonetheless, our approach can still be applied to cluster-based WSNs with static clusters, where data are aggregated by clusters before being relayed [24]. 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 subnetwork; after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a subnetwork 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.

2.1.2 Authentication Requirements

Though a specific application may determine whether data encryption is needed, TARF requires that the packets are properly authenticated, especially the broadcast packets from the base station. The broadcast from the base station is asymmetrically authenticated so as to guarantee that an adversary is not able to manipulate or forge a broadcast message from the base station at will. Importantly, with authenticated broadcast, even with the existence of attackers, TARF may use TrustManager (Section 3.4) and the received broadcast packets about delivery information to choose trustworthy path by circumventing compromised nodes. Without being able to physically capturing the base station, it is generally very difficult for the adversary to manipulate the base station broadcast packets which are asymmetrically authenticated. The asymmetric authentication of those broadcast packets from the base station is crucial to any successful secure routing protocol. It can be achieved through existing asymmetrically authenticated broadcast schemes that may require loose time synchronization.

2.1.3 Goals

TARF mainly guards a WSN against the attacks misdirecting the multihop routing, especially those based on identity theft through replaying the routing information. This paper does not address the denial-of-service (DoS) [3] 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: High 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. In our evaluation, throughput at a moment is computed over the period from the beginning time (0) until that particular moment. Note that single-hop retransmission may happen, and that duplicate packets are considered as one packet as far as throughput is concerned. Throughput reflects how efficiently the network is collecting and delivering data. Here, we regard high throughput as one of our most important goals.

Energy efficiency and 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. Note that link-level retransmission should be given enough attention when considering energy cost since each retransmission 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.

Scalability and 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. Here, we do not include other aspects such as latency, load balance, or airness. Low latency, balanced network load, and good fairness requirements can be enforced in specific routing protocols incorporating TARF.

2.2 EXISTING SYSTEM

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.

2.2.1 DISADVANTAGES

- Pocket losses.
- It doesn't reduce the high traffic level of data's.
- Capability of data transferring level is low.

2.3 PROPOSED SYSTEM

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.

2.3.1 ADVANTAGES

- It finds out the attacks in specifically so we can give clear solution of the network attacks
- It makes the Alternate path of transfer the data.
- It avoids the Packet losses.
- It Reduce the traffic level of transfer the data.

2.4 ARCHITECTURE DIAGRAM

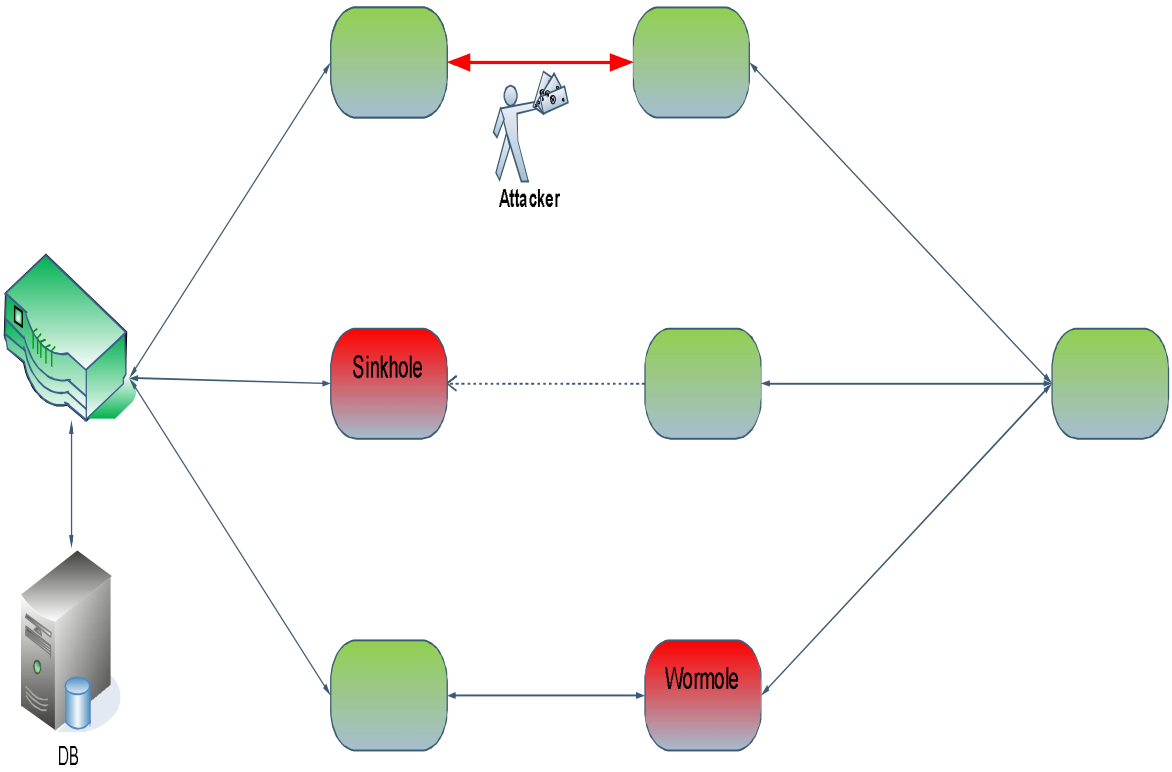

Fig 1 ARCHITECTURE DIAGRAM

2.5 USECASE DIAGRAM

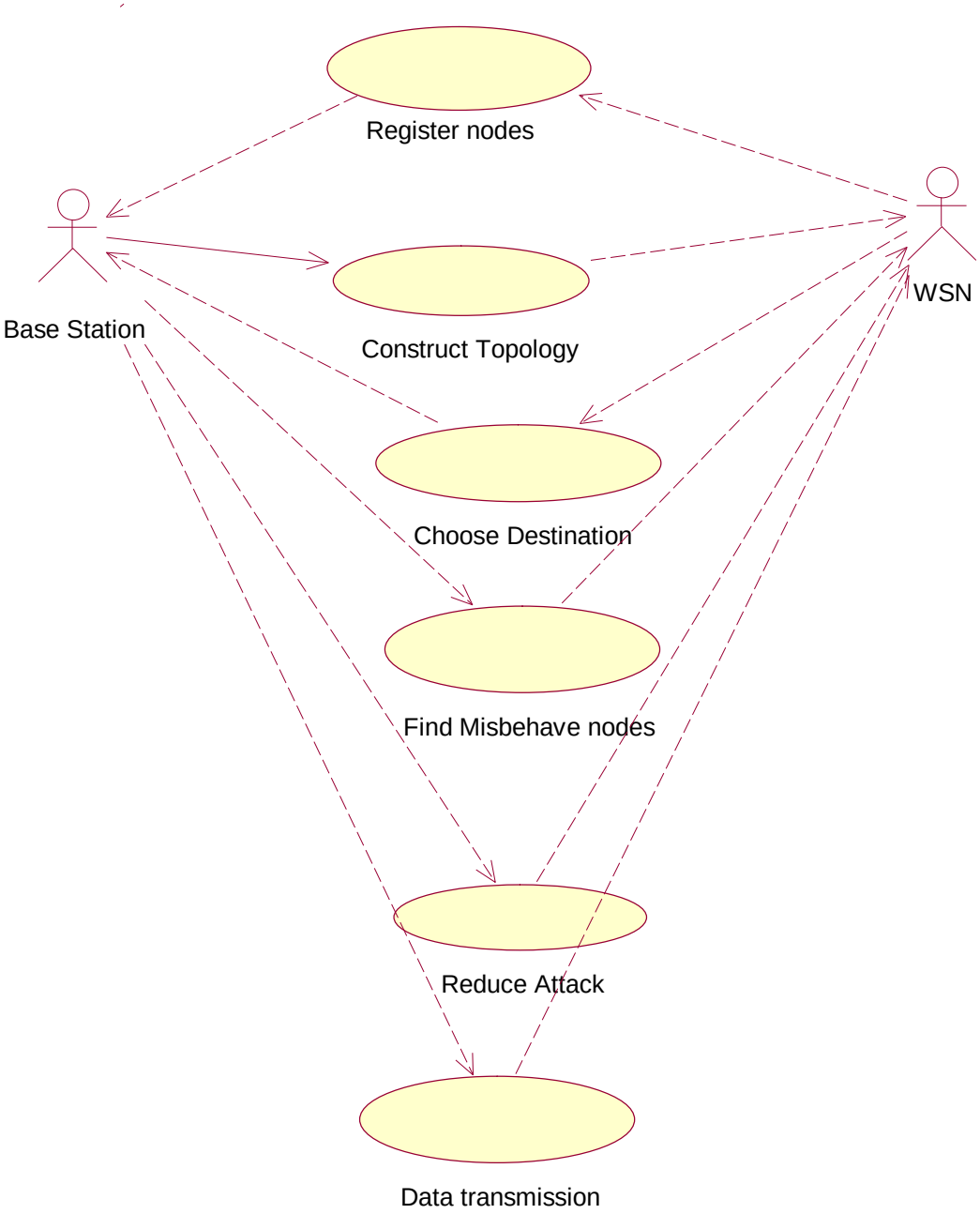

Fig 2 USECASE DIAGRAM

III. CONCLUSION

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.

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 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.

We have implemented a ready-to-use Tinos 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 ant detection mechanism that indicates the potential of TARF in WSN applications.

ACKNOWLEDGEMENT

I sincerely thanks to all authors in reference section. All papers in the reference section are very useful for my proposal. Their concepts, algorithms and techniques are very useful for my research.

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] W. Xue, J. Aiguo, and W. Sheng, “Mobile Agent Based Moving Target Methods in Wireless Sensor Networks,” Proc. IEEE Int’l Symp. Comm. and Information Technology (ISCIT ’05), vol. 1, pp. 22- 26, 2005.
[3] 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.
[4] 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.
[5] Z. Yan, P. Zhang, and T. Virtanen, “Trust Evaluation Based Security Solution in Ad Hoc Networks,” Proc. Seventh Nordic Workshop Secure IT Systems, 2003.
[6]K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, To appear in Journal of Ad Hoc Networks.
[7]R. Anderson, H. Chan, A. Perrig, Key infection: smart trust for smart dust, In 12th IEEE International Conference on Network Protocols, Berlin, Germany, October 2004.

[8]U.A.F. ARGUS Advanced Remote Ground Unattended Sensor Systems, Department of Defense, Argus, http://www.globalsecurity.
[9] C. Cachin, J.A. Poritz, Secure intrusion-tolerant replication on the internet, In IEEE International Conference on Dependable - Systems and Networks (DSN'02), Washington DC, USA, June 2002.
[10]. Carlson, R. Han, S. Lao, C. Narayan, S.S. ghani, Rapid prototyping of mobile input devices using wireless sensor nodes, In WMCSA'03, Monterey, CA, USA, October 2003.

