INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1086-1090
RECEIVED : 05/06/2016. PUBLISHED : 21/06/2016
June 21, 2016

INTRUSION DETECTION SYSTEM - A FRAMEWORK FOR WSNS

[1]R.Divya, [2]A.Sudhakar
[1]PG Student, Department of Computer Science Engineering, Bharathidasan Engineering College, Vellore,
[2]Assistant Professor, Department of Computer Science Engineering, Bharathidasan Engineering College, Vellore.

Abstract:
To secure the WSNs against adversaries misdirecting the multihop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. As such, we devise an estimation scheme based on ambient noise floor and validate it with real-world experiments. To further reduce estimation errors, we define an evaluation feedback metric to quantify the estimation errors and formulate jammer localization as a nonlinear optimization problem, whose global optimal solution is close to jammers' true positions. We explore several heuristic search algorithms for approaching the global optimal solution, and our simulation results show that our error-minimizing-based framework achieves better performance than the existing schemes. In addition, our error-minimizing framework can utilize indirect measurements to obtain a better location estimation compared with prior work.

Key words—Wireless sensor networks, routing protocols, security.

1. INTRODUCTION

Wireless sensor networks are spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The

propagation technique between the hops of the network can be routing or flooding. 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 [3]. 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. RELATED WORK

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.

3. PROPOSED SYSTEM:

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 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.

- Protect WSNs from the harmful attacks exploiting the replay of routing information
- Centres on trustworthiness and energy efficiency

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1086-1090
RECEIVED : 05/06/2016. PUBLISHED : 21/06/2016
June 21, 2016

- Allow existing routing protocols to incorporate our implementation
- No tight time synchronization & known geographic information

ADVANTAGES:

- Avoid disturbance of network communication
- Accuracy of the estimated locations.
- Improved network capacity.
- High in energy efficiency and reliable.

4. ARCHITECTURE DESIGN

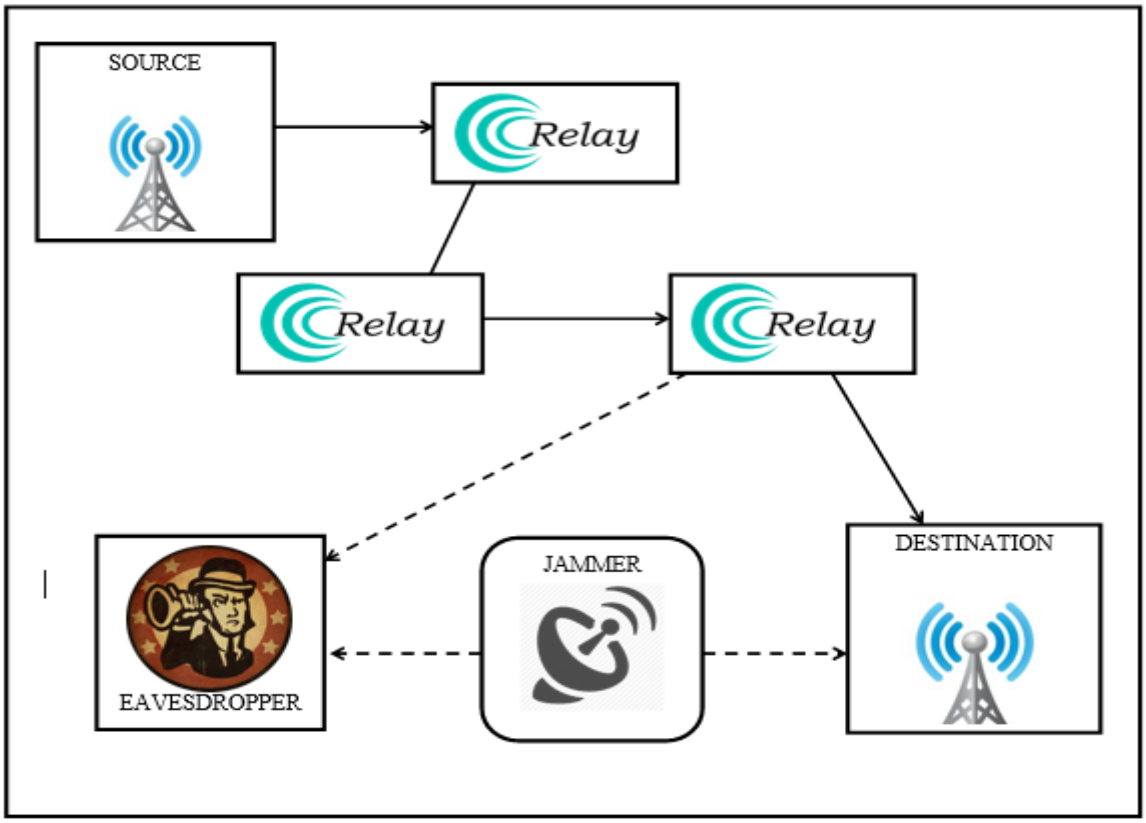

Fig.1.Architecture diagram

5. RESULT ANALYSIS

The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node S wishing to send a packet to a destination D obtains a source route to D. To perform a Route Discovery, the source node S broadcasts a ROUTE REQUEST packet that is flooded through the network in a controlled manner and is answered by a ROUTE REPL Y packet from either the destination node or another node that knows a route to the destination. To reduce the cost of Route Discovery, each node maintains a cache of source routes it has learned or overheard, which it aggressively uses to limit the frequency and propagation of ROUTE REQUESTs. Route Maintenance is the mechanism by which a packet' s sender S detects if the network topology

has changed such that it can no longer use its route to the destination D because two nodes listed in the route have moved out of range of each other. When Route Maintenance indicates a source route is broken, S is notified witha ROUTE ERROR packet. The sender S can then attempt to use any other route to D already in its cache or can in voke Route Discovery again to find a new route. Implementation Decisions Using the suggestions from the published description of DSR [10], we have optimized our implementation in a number of ways. Although the DSR protocol supports unidirectional routes, IEEE 802.11 requires an RTS/CTS/Data/ACK exchange for all unicast packets, limiting the routing protocol to using only bidirectional links in delivering data packets. We implemented DSR to discover only routes composed of bidirectional links by requiring that a node return all ROUTE REPL Y messages to the requestor by reversing the path over which the ROUTE REQUEST packet came. Nodes operate their network interfaces in promiscuous mode, disabling the interface' s address filtering and causing the network protocol to receive all packets that the interface overhears. These packets are scanned for useful source routes or ROUTE ERROR messages and then discarded. This optimization allows nodes to learn potentially useful information, while causing no additional overhead on the limited network bandwidth. Furthermore, when a node overhears a packet not addressed to itself, it checks the unprocessed portion of the source route in the packet' s header. If the node's own address is present, it knows that this source route could bypass the unprocessed hops preceding it in the route. The node then sends a gratuitous ROUTE REPL Y message to the packet' s source, giving it the shorter route without these hops. Finally, when an intermediate node forwarding a packet discovers that the next hop in the source route is unreachable, it examines its route cache for another route to the destination. If a route exists, the node replaces the broken source route on the packet with the route from its cache and retransmits the packet. If a route does not exist in its cache, the node drops the packet and does not begin a new Route Discovery of its own.

CONCLUSION

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

1. Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geo-graphic information.
2. The resilience and scalability of TARF are proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves both static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

REFRENCES:

[1] G. Zhan, W. Shi, and J. Deng, "Tarf: A Trust-Aware Routing Framework for Wireless Sensor Networks," Proc. Seventh European Conf. Wireless Sensor Networks (EWSN '10), 2010.
[2] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004.

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

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

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

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

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Conf. Information Processing in Sensor Networks (IPSN '04), Apr. 2004.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance Analysis of Mobile Agent-Based Wireless Sensor Network," Proc. Eighth Int'l Conf. Reliability, Maintainability and Safety (ICRMS '09),
pp.16-19, 2009.

[9] L. Zhang, Q. Wang, and X. Shu, "A Mobile-Agent-Based Middleware for Wireless Sensor Networks Data Fusion," Proc. Instrumentation and Measurement Technology Conf. (I2MTC '09), pp. 378-383, 2009.