International Journal of Applied Engineering and Technology ISSN: 2277-212X (Online)
An Open Access, Online International Journal Available at http://www.cibtech.org/jet.htm
2014 Vol. 4 (3) July-September, pp.45-49/Kapoor and Singh
Research Article

DESIGN & DEVELOPMENT OF ROBUST FRAMEWORK FOR ENERGY EFFICIENT ROUTING PATH FOR SECURE DATA TRANSMISSION

***Suman Kapoor and Parminder Singh**
ECE Department, Doaba College of Engineering and Technology
**Author for Correspondence*

ABSTRACT
The multi-hop routing in wireless sensor networks offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful attacks against the routing protocols, including sinkhole attacks, wormhole attacks and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Cryptography techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the wireless sensor networks against adversaries misdirecting the multi-hop routing, we have designed and implemented TARF (Trust-aware routing framework) for dynamic WSNs. Without tight time synchronization or known geographic information, it provides trustworthy and energy-efficient route. It proves effective against those harmful attacks developed out of identity deception.

Keywords: *TARF, Cryptography, WSN, Multi-Hop Routing*

INTRODUCTION
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. 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, which is known as a wormhole attack.
A node in a WSN 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. It may drop packets received, forward packets to another node not supposed to be in the routing path, or form a transmission loop through which packets are passed among a few malicious nodes infinitely.
Sinkhole attacks can be launched after stealing a valid identity, in which 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.
Most existing routing protocols for WSNs either assume the honesty of nodes or 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.
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

Related Works
Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It is about constructing and analyzing protocols that overcome the influence of adversaries and

which are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation (Zhan *et al.*, 2010).

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security. We present a suite of security building blocks optimized for resource constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and TESLA. SNEP provides the following important baseline security primitives: Data confidentiality, two-party data authentication, and data freshness (Zhao and Guibas, 2004).

Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side Ioannis Krontiris, Thanassis Giannetsos, One of the reasons that the research of intrusion detection in wireless sensor networks has not advanced significantly is that the concept of "intrusion" is not clear in these networks. In this paper we investigate in depth one of the most severe attacks against sensor networks, namely the sinkhole attack, and we emphasize on strategies that an attacker can follow to successfully launch such an attack (Wood and Stankovic, 2002).

We consider routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. We propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks — sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols (Karlof and Wagner, 2003).

Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack, where a node illegitimately claims multiple identities. This paper systematically analyzes the threat posed by the Sybil attack to wireless sensor networks (Jain and Kandwal, 2009).

We introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In our design, we leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16{32 bytes of overhead (Krontiris *et al.*, 2008).

Input Parameter

Neighbor Nodes

The neighbor nodes of the source nodes are taken into consideration while creating multi paths. For a our algorithm-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.

Trust Value

That trust level is denoted as T. Trust value is assigned for each and every node, the numeric value such as 0 or 1 is assigned, whereas 0 is considered to be malicious node and trust value 1 is considered to be normal node. Based upon the assigned trust value, the routing path is constructed. The node, which has trust value 1, will be included in the route rather than the node having trust level 0.

Energy Value

Energy cost is denoted as E. Energy value is assigned for each and every node, the numeric value such as 1, 2, 3 is assigned, whereas 1 is considered to be less energy consumption rather than 2 or 3. Based upon the assigned energy, the routing path is constructed. The node, which acquires less energy, will be included in the route rather than the higher energy consumption.

Step

Step 1: Deploy 'N' number of nodes in the wireless sensor network
Step 2: Arrange the nodes as a cluster
Step 3: Choose source node 'S' and destination node as base station "BS"
Step 4: Create TCP/UDP connection among the nodes
Step 5: Declare Energy value 'E' for all nodes in the network
Step 6: Declare trust value 'T' for All nodes in the network
Step 7: Create Routing Table, one- hop neighbor for all nodes deployed in WSN
Step 8: Create Routing path
Step 9: Start the packet delivery by using the router derived above
Step 10: Destination, Base station receives packet from source using Our Algorithm enable mode

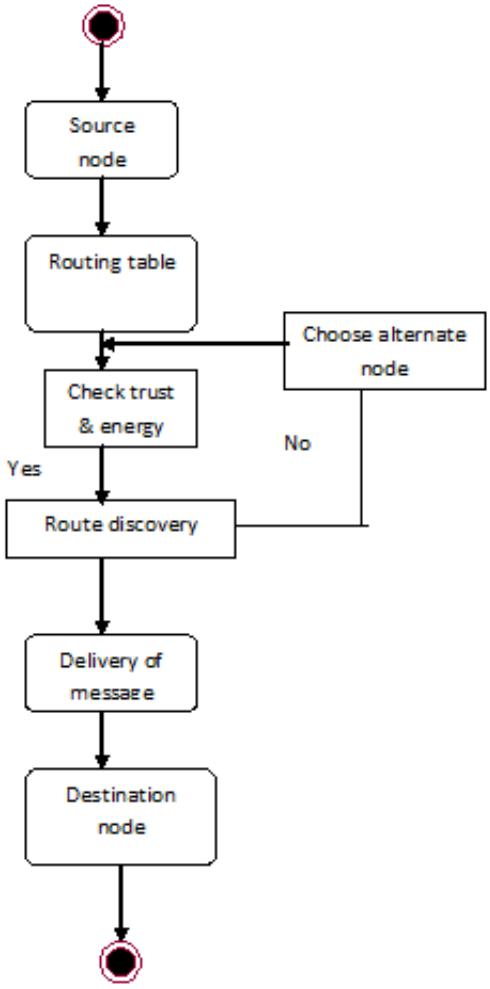

Figure 1: Activity Diagram

RESULTS AND DISCUSSION

Routing table in shown in the terminal, which shows the one- hop neighbor for all the nodes are arrived. The figure shows the one hop neighbor from node 0 to node 3.

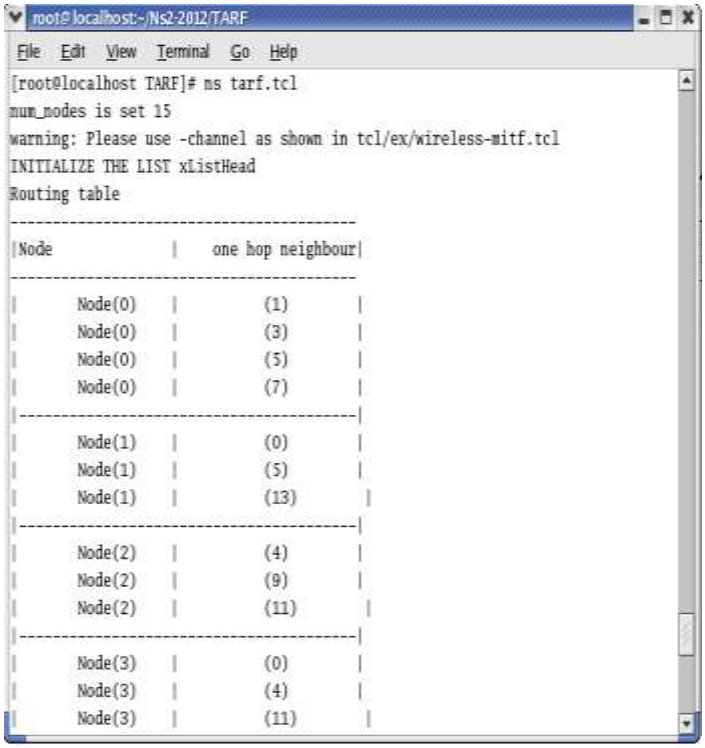

Figure 2: Snapshot of the program

Conclusion

Designed and implemented OUR ALGORITHM, a robust trust aware routing framework for WSNs, to secure multihop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. OUR ALGORITHM 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, OUR ALGORITHM 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, OUR ALGORITHM 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 OUR ALGORITHM are 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.

REFERENCES

Bai L, Ferrese F, Ploskina K and Biswas S (2009). Performance Analysis of Mobile Agent-Based Wireless Sensor Network. *Proceeding of Eighth International Conference on Reliability, Maintainability and Safety (ICRMS '09)* 16-19.

Jain M and Kandwal H (2009). A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks. *Proceeding of International Conference on Advances in Computing, Control, and Telecommunication Technologies* (ACT '09) 555-558.

Karlof C and Wagner D (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Proceeding of First IEEE International Workshop on Sensor Network Protocols and Applications.*

Krontiris I, Giannetsos T and Dimitriou T (2008). Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. *Proceeding of IEEE International Conference on Wireless and Mobile Computing, Networking and Communication* (WIMOB '08) 526-531.

Newsome J, Shi E, Song D and Perrig A (2004). The Sybil Attack in Sensor Networks: Analysis and Defenses. *Proceeding of Third International Conference on Information Processing in Sensor Networks* (IPSN '04).

Wood A and Stankovic J (2002). Denial of Service in Sensor Networks. *Computer* **35**(10) 54-62.

Xue W, Aiguo J and Sheng W (2005). Mobile Agent Based Moving Target Methods in Wireless Sensor Networks. *Proceeding of IEEE International Symposium on Communications and Information Technology* (ISCIT '05) **1** 22- 26.

Zhan G, Shi W and Deng J (2010). Our Algorithm: A Trust-Aware Routing Framework for Wireless Sensor Networks," *Proceedings of the 7th European Conference on Wireless Sensor Networks (EWSN '10)*.

Zhang L, Wang Q and Shu X (2009). A Mobile-Agent-Based Middleware for Wireless Sensor Networks Data Fusion. *Proceeding of Instrumentation and Measurement Technology Conference* (I2MTC '09) 378-383.

Zhao F and Guibas L (2004). Wireless *Sensor Networks: An Information Processing Approach* (Morgan Kaufmann).