Advance Research in Electrical and Electronic Engineering (AREEE)
Print ISSN : 2349-5804; Online ISSN : 2349-5812; Volume 2, Number 5; April – June, 2015 pp 4 – 7
Krishi Sanskriti Publications
http://www.krishisanskriti.org/AREEE.html

Energy Conserve & Protected Multi-hop Routing Protocols in Dynamic Wireless Sensor Networks (WSNs)

Narendra N. Tidke[1] and Sunita Jadhav[2]

PG Student, Department of Electronics & Telecommunication, Saraswati College of Engineering, Mumbai University
E-mail: [1]narendrantidke@gmail.com, [2]smj311972@gmail.com

Abstract—*Multi-hop routing in wireless sensor networks (WSNs) offer small protection against trickery throughout replaying routing information. A challenger can develop this defect to launch various harmful or even devastating attacks against the routing protocols, including wormhole attacks, sinkhole attacks and Sybil attacks. Conventional cryptographic techniques or efforts at mounting trust-aware routing protocols do not effectively address these problems. TARF demonstrates effective adjacent to those harmful attacks developed out of identity trickery; the flexibility of TARF is verified through extensive assessment with both simulation and observed experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. To secure the wireless sensor networks against adversaries misdirecting the multi-hop routing, we have proposed TARF, a robust trust-aware routing framework for dynamic WSNs. Without prolonged time synchronization or known geographic information, TARF offers dependable and energy-efficient route. We have put into action a low-overhead TARF module in TinyOS; this implementation can be included into existing routing protocols with the least effort. Based on TARF, we also verified a proof-of-concept mobile target detection application that functions well next to an anti-detection mechanism.*

Keyword: *Wireless sensor networks, routing protocols, security, TARF, Energy Cost.*

1. INTRODUCTION

These Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs were initially designed to facilitate military operations but its application has since been extended to health, traffic, and many other consumer and industrial areas. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path.

However multi-hop routing of wireless sensor nodes is the target for adversaries attacks. The attacker node can create the traffic collision with performing the valid transmission, they may tamper the nodes physically, they may jam the channel, they may drop or misdirect the data while routing. Based on the identity deception, the attacker node is able to perform some attacks on the nodes which are participating in multi-hop routing such as, selective routing, sink hole attack[4], worm hole attack[3], Sybil attack[8][5]. These networks have been subjected to numerous attacks among which Sinkhole attack is one of the notable ones.

The harmful and easy-to –implement attack is wormhole attack, in which an attacker node simply replays all the data packets which are under the routing process from the valid node to gain the latter nodes identity so that next time he can use that forged identity to participate in the network easily. 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 [6], [7], [9], [10], 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.

2. DESIGN CONSIDERATIONS

2.1. Assumptions

In this objective is secure routing for data collection tasks, which are one of the mainly fundamental functions of wireless sensor networks. In a data compilation task, a sensor node sends its example data to a remote base station with the help of other intermediate nodes, then there could be more than one base station, the direction-finding approach is not affected by the number of base stations that there is only one base station. An opponent may fake the identity of any legal node through replaying that node's outgoing routing packets and spoofing

the acknowledgement packets, even remotely through a wormhole. In addition, to merely simplify the introduction of TARF to assume no data aggregation is involved.

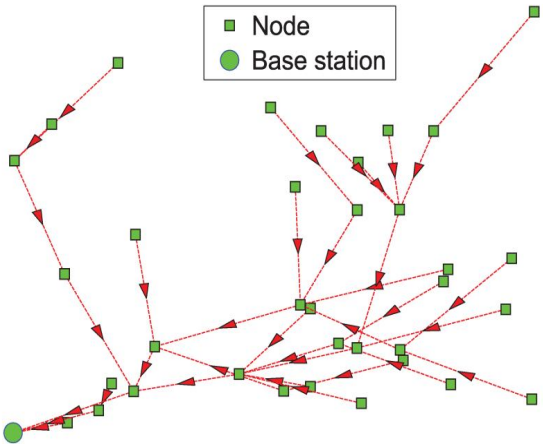

Fig. 2.1: Multi-hop routing for data collection of a WSN.[1].

It is to be applied to cluster based wireless sensor networkss with static clusters, where data are cumulatively by clusters before being relayed. Cluster-based wireless sensor networkss allows for the great savings of energy and bandwidth through aggregating data from children nodes and performing routing and transmission for children nodes. The framework can be functional to this sub-network to achieve secure routing for cluster based wireless sensor networkss. 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 child nodes, even if any link-level security features may be further employed.

2.2. Authentication Requirements

Though a specific application may determine whether data encryption is needed, TARF requires that the packets are correctly authenticated, particularly the broadcast packets from the base station. The transmition from the base station is unevenly authenticated so as to guarantee that an adversary is not able to manipulate or forge a broadcast message from the base station at will. With authenticated broadcast, even with the existence of attackers, TARF may use TrustManager and the received broadcast packets about delivery information to choose trustworthy path by circumventing compromised nodes. Without being able to capturing the base station, it is generally very difficult for the opposition to manipulate the base broadcast packets from the base station is critical to any successful secure routing protocol. It can be achieved through existing irregularly authenticated broadcast schemes that may require loose time synchronization. As an example, µTESLA achieves asymmetric authenticated broadcast through a symmetric cryptographic algorithm and a loose delay schedule to disclose the keys from a key chain.

3. DESIGN OF TARF

TARF secures the multi-hop routing in wireless sensor networkss against intruders developing the repetation of routing information by evaluating the trustworthiness of neighboring nodes. It recognizes such intruders that misdirect obvious network traffic by their low trust advantage and routes data through paths circumventing those intruder to achieve reasonable throughput. TARF is also energy-efficient, highly scalable, and well flexible. Before introducing the detailed design, we initially introduce several essential notions here.

Neighbor: For a nodeN, a neighbor (neighboring node) of N is a node that is reachable from N with one-hop wireless transmission.

Trust level: For a node N, the trust level of a neighbor is a decimal number in [0, 1], representing N's opinion of that neighbor's level of trustworthiness. Particularly, the trust level of the neighbor is N's estimation of the probability that this neighbor correctly delivers data received to the base station. That trust level is indicates as T.

Energy cost: For a node N, the energy cost of a neighbor is the average energy cost to successfully deliver a unit-sized data packet with this neighbor as its next-hop node, from N to the base station. This energy cost is indicated as E.

3.1. Routing Procedure

TARF with as many other routing protocols, runs as a interrupted service. The length of that phase determines how regularly routing information is exchanged and reorganized. The achievement of the base station broadcast triggers the exchange of energy report in this new period. henever a node receives such a broadcast message from the base station, it recognizes that the most recent period has ended and a new period has just started. No fixed time synchronization is required for a node to keep track of the beginning or ending of a period. During each period, the Energy Watcher 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 locality table.

3.2. ENERGY WATCHER

A node N's EnergyWatcher computes the energy cost ENb for its neighbor b in N's neighborhood table and how N decides its own energy cost EN. Before going further, The cost caused by one-hop retransmissions should be included when computing ENb. Suppose N decides that A should be its next-hop node after comparing energy cost and trust level. Then N's energy cost is EN = ENA. Denote EN!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:

$$ENb = EN!b + Eb \quad (1)$$

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 of one hop transmissions from N to b are independent with the same probability psucc of being acknowledged, we first compute the average number of one-hop sending is needed before the acknowledgement is received as follows:

$$\Sigma_{i=1}^{\infty} i \cdot psucc \cdot (1 - psucc)^{i-1} = \frac{1}{psucc} \quad (2)$$

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 neighborhood 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. 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.

4. IMPLEMENTATION AND EMPIRICAL EVALUATION

In order to estimate TARF in a real-world setting, we execute the TrustManager component on TinyOS 2.x, which can be included into the existing routing protocols for wireless sensor networks with the least attempt. We implemented TARF as a self-contained routing protocol on TinyOS 1.x before this second implementation.

4.1. TrustManager Implementation Details

The Trust Manager component in TARF is enfolded into an self-determining TinyOS configuration named TrustManagerC. Although it is possible to implement TARF with a period always synchronized with the routing protocol's period that would cause much intrusion into the source code of the routing protocol. The current TrustManagerC utilizes a period of 30 seconds; for exact applications, by adjusting a convinced header file, the period extent may be re-configured to reflect the sensing occurrence, the energy effectiveness and trustworthiness requirement.

4.2 TARF implementation Details

This new implementation integrating TARF requires moderate program storage and memory utilization. Here implemented a typical TinyOS data collection application, Multihop Oscilloscope, based on this new protocol. The Multihop Oscilloscope application, with certain modified sensing parameters for our later evaluation purpose, sometimes makes sensing samples and sends out the sensed data to a root via multiple routing hops. Originally, Multihop Oscilloscope uses CTP as its routing protocol. Now list the ROM size and RAM size necessity of both implementation of Multihop Oscilloscope on non-root Telosb motes. The enabling of TARF in Multihop Oscilloscope increases the size of ROM by around 1.3KB and the amount of memory by around 1.2KB.

4.3 Trust Table Updated

Once again trust table is updated as shown in Fig. 4.1. This time the chosen path is L1-L2-L3-L4-L5-L10-Base Station. The Source Node L1 will update the trust value of node L10 to 0.6 which was initially 0.5 (Trust Value is initializing 0.7).

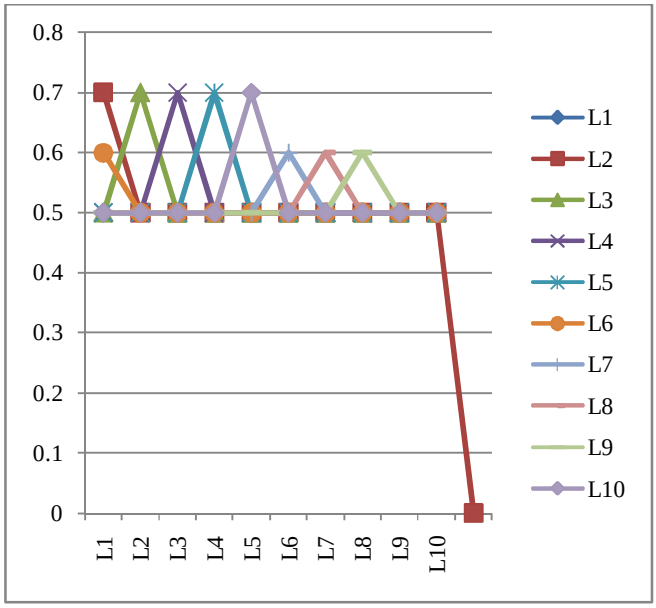

Fig. 4.1: Graph based on trust value for the new path (L1-L2-L3-L4-L5-L10-Base Station).

Graph Based On Trust Value :- represents the graph based on trust value for the new path. As there is no attacker this path will be chosen by Source Node L1 for file transfer.

5. CONCLUSIONS AND FUTURE WORK

Trust Aware Routing Framework (TARF), can be used 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. TARF effectively protects WSNs from severe attacks through replaying routing information.

TARF is designed to guard a WSN against the attacks misdirecting the multi-hop routing, especially those based on identity theft through replaying the routing information. Other types of attacks such as the denial-of-service (DoS) attacks are left as future enhancement. Also we do not address the attacks of injecting into the network a number of data packets containing false sensing data but authenticated (possibly through hacking). That type of attacks aim to exhaust the network resource instead of misdirecting the routing.

6. ACKNOWLEDGEMENT

It is a pleasure to acknowledge the assistance of my guide **Prof. Sunita Jadhav,** Assistant Professor, Department of Electronics and Telecommunication Engineering, Saraswati college of engineering, Mumbai, for his valuable guidance, continuous support and advice and constant encouragement throughout my project work. I am also grateful to **Prof. Mandeep Kaur**, Head, Department of Electronics and Telecommunication Engineering Saraswati college of engineering,Mumbai university for his last minute instructions which helped me to focus my work in the right directions.

I would like to extend my gratitude to honorable

Dr. Manjusha Deshmukh Principal of Saraswati college

of engineering,Mumbai, for being a constant source of inspiration.

Finally, I would like to extend my thanks to all those who have contributed, directly or indirectly to make this project successful.

REFERENCE

[1] Guoxing Zhan, Weisong Shi, "Design and Implementation of TARF: Trust-Aware Routing Framework for WSNs" IEEE Transactions On Dependable And Secure Computing, vol. 9, no. 2, March/April 2012

[2] G. Zhan, W. Shi, and J. Deng, "Design, implementation and evaluation of tarf: A trust-aware routing framework for dynamic wsns," http://mine.cs.wayne.edu/_guoxing/tarf.pdf, Wayne State University, Tech. Rep. MIST-TR-2010-003, Oct. 2010.

[3] M. Jain and H. 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.

[4] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB ¨08), 12-14 2008, pp. 526 –531.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in Proc. of the 3rd International Conference on Information Processing in Sensor Networks (IPSN¨04), Apr. 2004.

[6] L. Bai, F. Ferrese, K. Ploskina, and S. 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.

[7] 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.

[8] 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.

[9] W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based moving target methods in wireless sensor networks," in IEEE International Symposium on Communications and Information Technology (ISCIT 2005), vol. 1, 12-14 2005, pp. 22 – 26.

[10] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in Proceedings of the 10th International Conference on Advanced Communication Technology (ICACT 2008), vol. 1, 17-20 2008, pp. 75 –78.

[11] A. Rezgui and M. Eltoweissy, "Tarp: A Trust-Aware Routing Protocol for Sensor-Actuator Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '07), 2007.

[12] A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, pp. 2826-2841, Oct. 2007.

[13] S. Chang, S. Shieh, W. Lin, and C. Hsieh, "An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 311-320, 2006.