International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 1 –JULY 2014.

Energy Efficient and Secure, Trusted framework for Wireless Sensor Networks

Sriramula SriPujitha[#1] and SubbaRao.k[*2]

[#]PG Scholar (M.Tech-IT), LakkiReddy BaliReddy College of Engineering, Mylavaram, India
[*]Associate Professor (Dept., of IT), LakkiReddy BaliReddy College of Engineering, Mylavaram, India
[1]sspujitha66@gmail.com
[2]ksubbarao_22@yahoo.co.in

Abstract- The area of Wireless Sensor Networks (WSNs) applications is increasing widely over the last few years. As this new type of networking is characterized by severely constrained node resources, limited network resources and the requirement to operate in an ad hoc manner, implementing security functionality to protect against adversary nodes becomes a challenging task. While routing Wireless Sensor nodes in the Multi-hop network, nodes may undergo some attacks such as sink hole attack, worm hole attack, Sybil attack etc., by the attackers through identity deception. So, to secure WSN's against attackers or hackers misdirecting the nodes in the network while routing, in our base paper we have designed and implemented TARF, a robust trust aware routing framework concept for dynamic for WSN's. TARF provides trustworthy and energy-efficient route and also it provides security against all these attacks which are mentioned above.

Keywords: Wireless sensor network, routing protocols, security, Sinkhole attack, wormhole attack, Sybil attack.

I. INTRODUCTION

Wireless sensor network (WSN) refers to a group of distributed 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[6], worm hole attack[5], Sybil attack[4][7]. These networks have been subjected to numerous attacks among which Sinkhole attack is one of the notable ones.

In Sinkhole attack, sometimes the adversary node poses itself as a fake base station (BS) and receives all data of the network. It prevents data from reaching the main BS, or changes the received data and then transfers them to the main BS. In the Sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical Sinkhole with the adversary at the center. 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. Soon after the attacker stealing the identity he can misdirect the network traffic such as, 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. Using same technique as in case of sinkhole attack we can have one more strong attack called Sybil attack.

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 [8], [9], [10], [11], 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. As for as WSN‟s 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.

II. Related works

Wireless sensor networks (WSNs) [2] are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. We discuss more related work here in addition to the introduction in Section 1. It is generally hard to protect WSNs from wormhole attacks, sinkhole attacks and Sybil attacks based on identity deception. In [1], 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. In [3], this paper has presented an alternative method to confirm the trustworthiness of nodes in WSN. In this scheme involves designing a trusted platform and an energy efficient authentication protocol. The trusted mechanism has contributes to enhance security in WSNs by reducing the probability of fake or clone sensor node through non-regenerated unique platform identity.

It is generally hard to protect WSNs from wormhole attacks, sinkhole attacks and Sybil attacks based on identity deception. The countermeasures often requires either tight time synchronization or known geographic information. FBSR, as a feedback-based secure routing protocol for WSNs, uses a statistics-based detection on a base station to discover potentially compromised nodes. But the claim that FBSR is resilient against *wormhole* and *Sybil* attacks is never evaluated or examined; the Keyed-OWHC-based authentication used by FBSR also causes considerable overhead. There are certain existing secure routing solutions for WSNs based on trust and reputation management; however, they rarely address the "identity theft" exploiting the replay of routing information. Two such representative solutions are ATSR and TARP. Neither ATSR nor TARP offers protection against the identity deception through replaying routing information. ATSR is a location-based trust-aware routing solution for large WSNs. ATSR incorporates a distributed trust model utilizing direct and indirect trust, geographical information as well as authentication to protect the WSNs from packet misforwarding, packet manipulation and acknowledgements spoofing. Another trust-aware routing protocol for WSNs is TARP, which exploits nodes' past routing behavior and link quality to determine efficient paths.

III. Problem Statement

A. *EXISTING SYSTEM*

In Existing system, when the file send from base station in that situation hackers aggravated network conditions. A traditional cryptographic techniques effort does not address the severe problems. That time the file could be affected by hackers. So, the network will be damaged. 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.

Disadvantages:

1. There is no trusted authority to trust the nodes.
2. There is no Strong packet hiding methods for strong cryptography
3. No fixed routing instead Flooding in Routing will be there.
4. No Attack Finders are there.

B. *PROPOSED SYSTEM*

In Proposed System, focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighbouring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TARF is also energy-efficient, highly scalable, and well adaptable

IV. System Architecture

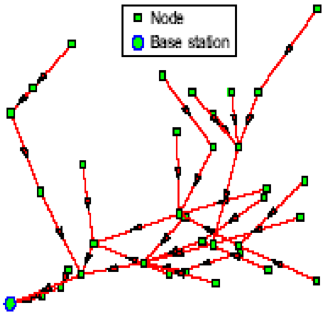

Fig. 1. Multi-hop routing for data collection of a WSN.

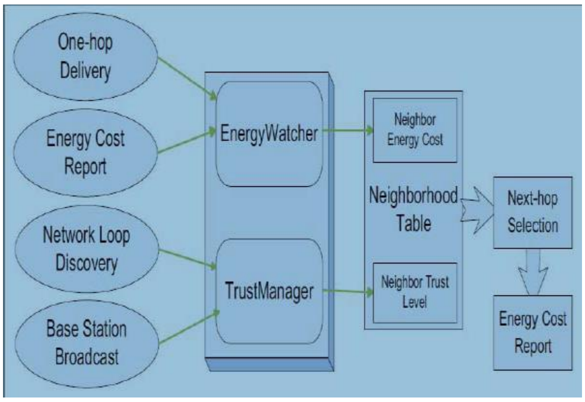

Fig. 2. A trust-aware routing framework for WSN's

Each node selects a next-hop node based on its neighbourhood table, and broadcast its energy cost within its neighbourhood. To maintain this neighbourhood table, Energy Watcher and Trust Manager on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbours.

V. Implementation

1) *Routing the Network*

In this module, the networks embedded on the physical fiber topology. However, assessing the performance reliability achieved independent logical links can share the same physical link, which can lead to correlated failures. Mainly, it focuses on assessing the reliability of energy level and trusted network.

2) *Transfer File*

In this module, Analysis the Shortest Path algorithm independently routes each logical link on a physical path with the minimum number of hops in trusted network basis. Hence, under the algorithm Shortest Path, each light- path greedily takes the most reliable route and transfers the file.

3) *Sinkhole and Wormhole Attacks*

i. Prevent the base station from obtaining complete and correct sensing data.
ii. Particularly severe for wireless sensor networks.
iii. Some secure or geographic based routing protocols resist to the sinkhole attacks in certain level.
iv. Many current routing protocols in sensor networks are susceptible to the sinkhole attack.

4) *Energy Watcher & Trust Manager*

In this module 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 sub-network, after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a sub-network consisting of the cluster headers. Our framework can then be applied to this sub-network to achieve secure routing for cluster based WSNs.

VI. Conclusion

Designed and implemented TARF, a robust trust aware routing framework for WSNs, to secure multihop 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 neighbours and thus to select a reliable route. This prospective has a noticeable impact on WSN for their strong energy efficiency, robustness and self configuration requirements.

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 static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

VII. References

[1] Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng, IEEE 2012 Transactions on Dependable and Secure Computing, Volume: 9 , Issue: 2:" Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs".

[2] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann Publishers, 2004.

[3] Yusnani Mohd Yussoff1, Habibah Hashim2 and Mohd Dani Baba, IEEE Transaction on Dependable and Secure Computing,Vol 13,Issue 4: Identity-based Trusted Authentication in Wireless Sensor Network

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.