© 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939

Overview of Trust-Aware Routing Framework of WSNs

Meenal N. Borikar,Priya R.Madavi ,Geeta N.Musale ,Tejaswini V.Potdukhe
Students,
Electronic and Telecommunication
Govt. College of Engg , Chandrapur, Maharastra,

***Abstract* - In wireless sensor networks (WSNs), the multi-hop routing procedure offers some kind of protection against identity deception through routing information. There are so many harmful attacks which distract information of routing protocols, such as *sinkhole* attacks, wormhole attacks and *Sybil* attacks. In wireless sensor networks (WSNs),the traditional cryptographic techniques are use for enhancing trust aware routing protocol but this technique do not detect such severe problem. So for protecting the WSNs against misdirecting the information during the multi-hop routing procedure, we developed and implement a protocol named as TARF, i.e. A trust aware routing framework for WSN. TARF provides a trustworthy and energy efficient path, without any help of tight time synchronization or geographic condition. TARF provide effective path during routing without any effect of harmful attacks. The property of recover the information which has been stretched during routing process of TARF is provide through both extensive simulation and empirical evolution with large scale WSNs. We have implemented a ready to use tiny-Os module of TARF with low overhead. This TARF can be implemented into exciting routing protocol with least efforts. Based on TARF, the concept of mobile target detection application in anti-detection mechanism is demonstrated.**

I. INTRODUCTION

Wireless sensor node send message to base station with a narrow bandwidth of radio communication range via multi hop path. However multi-hop path of wireless sensor network get affected by harmful attacks. An attacker may disturb the node setting physically, create traffic collision during valid transmission may lose or change the path of message while going towards destination or jam the communication channel. In this survey of routing protocol we focus on the attacks which causes traffic collision or destroys the information. Base on identity deception, it is difficult to know which attacks are occurs during routing, such as sinkhole attacks ,wormhole attacks and Sybil attack, etc. when a harmful attacks occur in malicious node misdirect the outgoing routing packets from valid to node fake node. This malicious node uses fake identity to participate in routing network. So due to the fake base station the packets which are received will be proceed further without original identity. The fake node will be transferred or divert information from true valid node to another node in network, this kind of attack is known as Wormhole attack.

Sinkhole attack are another kind of attack which will create after occurrence of fake base station, and that particular base station itself behave like a true base station. It control and proceed further routing process. This same method can create another strong attack known as Sybil attack.

In WSNs, as this attacks are occurred, there is a need of protocol which minimize this attacks by providing a trusted path for routing.

The following authors has research the routing Frame work for the Wireless sensor network. Each one has the following conclusion and the drawbacks.

1 An implementation framework for trajectory-based routing in ad hoc networks

In this paper, they studied various implementation issues of trajectory-based routing (TBR) for stateless routing in ad hoc networks.

They use to Bezier curves for defining trajectories in TBR. Various shapes for routes can be defined by using Bezier curves. They implemented different types of algorithms based on trajectories defined by Bezier curves. Also proposed an optimal forwarding algorithm, lowest deviation from curve (LDC),that obeys to trajectories the most. They work on extensive simulations in order to implement the performance of forwarding algorithms. They found that LDC is good for moderately populated ad-hoc networks. They also found that Random forwarding performs average while avoiding significant computational overhead. When the signaling phase introduced to the protocol they also found a methodology for extending TBR with Bezier curves to longer as well as more complicated trajectories, which can be encoded by larger information. They implemented a method enables routing of data packets via complex trajectories, by keeping the packet header size same.

Numerous work may be involve for implementation as well as for development of this method with a particular assumption provide for signaling overhead. Several issues remain to be investigated such as effect of mobility and traffic patterns. Also, future work includes studying methods for increasing resilience (i.e. probability of reaching to destination) for different forwarding algorithms.

Finally, they conclude how to route the packets when the destination and the source are mobile, is an open issue.

2. Efficient Greedy Geographical Non-Planar Routing with Reactive Deflection 2

During all this process a novel geographical routing scheme for spontaneous wireless mesh networks established. Greedy geographical routing has many advantages but having a disadvantage, i.e. there are losses of packets during routing process at the border of voids.

This paper shows that they invented a flexible greedy routing scheme, which can be used by any variant node of geographical routing and it can work for many connectivity graph, it is not necessary that the graphs should be Unit Disk graph. The motive of this scheme is to reactively detect voids, backtrack packets, and propagate information on blocked sectors to reduce packet loss. An extrapolating algorithm is used to reduce the latency of void discovery and to limit route stretching. The performance of this scheme via simulation shows that their modified greedy routing avoids most of packet losses.

Theyimplemented a scheme for greedy geographical routing with reactive defect detection. The focus of this scheme is to reactively detect jam, blocked nodes and propagate the defect information by computing a set of blocked nodes. To reduce the route length and accelerate void detection in dense mesh networks, they have also proposed a method to extrapolate void location.

Simulation results described decrease in packet loss as well as the route length compared to greedy routing.

3. Routing Techniques in Wireless Sensor Networks: A Survey3

During their survey related to routing techniques in WSNs they conclude that Routing in sensor networks is ainteresting area of research and rapidly growing set of research results. In this paper they presented a comprehensive survey of routing techniques in wireless sensor networks which have being illustrated in the literature.

They have the common objective of extending the lifetime of the sensor network, without compromising data delivery. All routing techniques are classified based on the network structure into three categories: flat, hierarchical, and location basedRouting protocols.

These protocols are further classified into multipath based, query based, negotiation based or QoS based routing techniques depending on the protocol operation. They also highlighted the design tradeoffs between energy and communication overhead saving in the routing ensamples, as well as, the advantages and disadvantages of each routing technique. They also notice that many of the routing techniques look promising but there are some challenges that need to be solved in the sensor networks. In this paper they highlighted those challenges, also pinpointed future research directions in that regards.

4. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection 4

In this paper, they proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects, namely, social trust and QoS trust. They developed a probability model utilizing stochastic Petri nets techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status. They illustrated the feasibility of dynamic hierarchical trust management and application-level trust most favorable design concepts with trust based geographic routing and trust-based IDS applications. The application performance of this protocol can be optimized by identifying the best way to form trust as they all use trust out of individual social and QoS trust properties at runtime.

The results indicated that our trust-based geographic routing protocol performs close to the ideal performance of flooding-based routing in delivery ratio and message delay without sacrificing much in message overhead compared with traditional geographic routing protocols which do not use trust. Our trust-based IDS algorithm performs traditional anomaly-based IDS techniques in the detection probability while maintaining sufficiently low false positives. There are many research directions, including (a) devising and validating a decentralized trust managementscheme for autonomous WSNs without base stations; (b) investigating the impact of the cluster size and the trust update interval to the protocol performance and lifetime of a given WSN; and (c) investigating the feasibility of applying hierarchical trust management to more dynamic networks such as mobile-WSNs, mobile cyber physical systems, or mobile ad-hoc networks (MANETs).

TARF effectively protects WSNs from severe attacks through replaying routing information; it does not requires tight time synchronization and known geographic information. The property of recovery the information which has been stretched during routing process of TARF is proved through both extensive simulation and empirical evaluation with large-scaleWSNs; the evaluation of TARF depends upon both static and dynamic settings, surrounding network conditions, as well as harmful attacks such as wormhole attacks and Sybil attacks. They have implemented a ready-to-use Tiny-OS module of TARF with low overhead.This TARF module can be implemented into existing routing protocols with the least effort, so it can produce secure and efficient fully-functional protocols. Finally, they demonstrate a proof-of-concept mobile target detection application that is built on top of TARF and is resilient in the presence of an anti-detection mechanism; that indicates the potential of TARF inWSN applications.

II. CONCLUSION

We have designed and implemented TARF, trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers, which diverts the routing information.

TARF focuses on trust factor and energy efficiency of neighboring nodes, which are very important for the survival of a WSN in a hostile environment. With the knowledge of trust management, TARF track a neighboring nodes depending on the trustworthiness of it and thus to select a efficient route. Our main objectives are listed as follows.

1. Unlike previous scheme of secure routing for WSNs, TARF effectively protects WSNs from harmful attacks which replaying routing information; it does not require any tight time synchronization or known geographic information.

2. The effectiveness of TARF is proved through both extensive simulation and empirical evaluation with large-scale WSNs, whereas evaluation involves both static and dynamic settings, hostile network conditions, as well as harmful attacks such as wormhole attacks and Sybil attacks.
3. We have implemented a ready-to-use Tiny OS module of TARF with low overhead, this TARF module can be implemented into existing routing protocols with the minimum effort, thus producing secure and efficient fully-functional protocols.
4. Finally, we prove the concept of mobile target detection application that is built on TARF and it is able to recover back in the presence of an anti-detection mechanism; that indicates the potential of TARF in WSN applications.

III. ACKNOWLEDGEMENTS

We are extremely grateful and remain indebted to our guide Prof. Dr. D.V.Rojatkar for being a source of inspiration and for his constant support in the Design, Implementation and Evaluation the project. We are thankful to them for their constant constructive criticism and invaluable suggestions, which beneted us a lot whiledeveloping the project on "SIMULATION OF TARFTURSTAWARE ROUTING FRAMEWORK FOR WSNs" .He has been a constant source of inspiration and motivation for hard work. He has been very co-operative throughout this project work. through this column, it would be our utmost pleasure to express our thanks to him for their encouragement, co-operative and consent without we might not be able accomplish this project. We also express our gratitude to our Prof.Dr.D.V.Rojatkar for providing us the infrastructure to carry out the project and to all staff members who were directly and indirectly instrument in enabling us to stay committed for the project.

REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, “Tarf: A trustawarerouting framework for wireless sensornetworks,” in *Proceeding of the 7th EuropeanConference on Wireless Sensor Networks(EWSN’10)*, 2010.

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

[3] A. Wood and J. Stankovic, “Denial of servicein sensor networks,” *Computer*, vol. 35, no. 10,pp. 54–62, Oct 2002.

[4] C. Karlof and D. Wagner, “Secure routing inwireless sensor networks: attacks andcountermeasures,” in *Proceedings of the 1st IEEEInternational Workshop on Sensor NetworkProtocols and Applications*, 2003.

[5] M. Jain and H. Kandwal, “A survey oncomplex wormhole attack in wireless ad hocnetworks,” in *Proceedings of InternationalConference 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 sensornetworks; the intruder side,” in *Proceedings ofIEEE International Conference on Wireless andMobile Computing, Networking andCommunications(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 anddefenses,” in *Proc. of the 3rd InternationalConference on Information Processing in SensorNetworks(IPSN’04)*, Apr. 2004.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas,“Performance analysis of mobile agent-basedwireless sensor network,” in *Proceedings of the8th International Conference on Reliability,Maintainability and Safety (ICRMS 2009)*, 20-242009, pp. 16 –19.