RELIABLE DATA TRANSMISSION IN WIRELESS NETWORK USING SECURE TRUST BASED ROUTING

Ms.M.Krishnaveni[1] , Dr.G.Selvakumar[2], Ms.S.Aruna Devi[3]

[1]P.G. Scholar Department of ECE, Muthayammal Engineering College, Tamilnadu, India.
[2]Professor, Department of ECE, Muthayammal Engineering College, Tamilnadu, India.
[3]Assistant Professor, Department of ECE, Muthayammal Engineering College, Tamilnadu,India.

---***---

Abstract - *Wireless networks are vulnerable to various network attacks. To cope with these security issues, trust-based routing schemes have emerged. Typically, trust routing schemes are mainly focused on detection of packet drop attacks, because this type of an attack is simple and obviously a malicious behavior. However, there are more advanced attacks, such as, false trust reporting or compromised attacks, where trust-based routing to defend these attacks is more difficult because of their ambiguous behavior. In order to ensure data transmission reliability even against such attacks, in this letter a Authenticated Anonymous secure routing scheme is proposed for wireless networks. Simulation results show that the AASR scheme provides a better performance compared to the ATR and SPR schemes. To protect these networks, security protocols have been developed to protect routing and application data. However, these protocols only protect routes or communication, not both. Both secure routing and communication security protocols must be implemented to provide full protection.*

Key Words: Trust Based Routing, Wireless Sensor Networks, Secure Path Routing, Security Protocols, Authenticated Anonymous Secure Routing.

1. INTRODUCTION

Wireless sensor networks (WSN) are collection of nodes where each node has its own sensor, processor, Transmitter and receiver. The sensors are low cost devices that perform a specific type of sensing event. Being of low cost such sensors are deployed densely throughout the area to monitor specific event. WSN are highly distributed networks of small lightweight wireless nodes. Sensor nodes are called as motes. It monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity etc. Sensor networks are widely applied in various filed such as environment monitoring, military applications, health care and home intelligence. The major issue in WSN is security requirements. One of the main issues is secure routing. Because of the wireless nature routing has to be done in secure way to avoid the information loss, and various attacks.

1.1 Related Work

conventional trust based routing schemes are focused on being adaptive to packet drop attacks, where these schemes are commonly based on distributed trust routing structures and are highly vulnerable to compromised attacks (e.g., good or bad-mouthing attacks) because they do not have any means to distinguish false trust information. Meanwhile, the trust evaluation scheme GlobalTrust was proposed to detect various network attacks accurately, which shows a high performance in malicious node detection. In this scheme, trust information of all nodes in the network are collected by the Trust Authority (TA), and the TA computes the global view based on the reputation of each node.

However, this scheme deals only with the trust calculation of the nodes, and does not deal with routing metrics or methods. Therefore, in this letter a centralized trust-based secure routing (CSR) scheme is proposed that enables secure routing based on routing path selection that avoids malicious node selections to maximize the paths trust level while supporting the required quality of service (QoS).

The pathradar is the component used for reputation Ratings are kept about every node in the network based on its routing activity and they are updated periodically. Node select routes with the highest average node rating. Thus, nodes can avoid misbehaving nodes in their routes as a response. The pathradar combines knowledge of misbehaving nodes with link reliability data to select the route most likely to be reliable. Specifically, each node maintains a rating for every other node it knows about in the network and calculates a path metric by averaging the node ratings in the path, enabling thus the selection of the shortest path in case reliability information is unavailable. Negative path values indicate the existence of one or more misbehaving nodes in the path. If a node is marked as misbehaving due to temporary malfunction or incorrect accusation, a second –chance mechanism is considered, by slowly increasing the ratings of nodes that have negative values or setting them to anon-negative values after a long-timeout. However, misbehaving nodes still transmit their packets as there is no punishment mechanism adopted here. Moreover, no second hand information propagation view is considered which limits the cooperativeness among nodes.

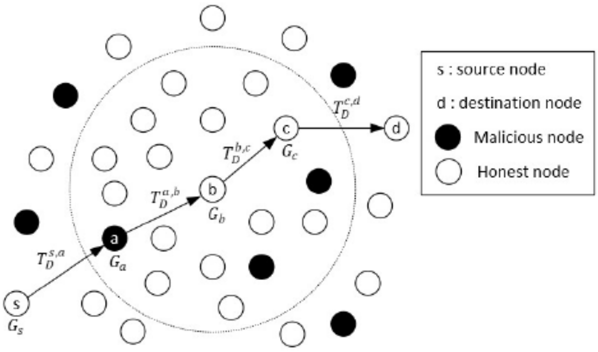

Figure 1.1 Finding Trust Node

2. EXISTING SYSTEM

The existing systems are available for trust node identification and secure routing are discussed. It discuss with the different techniques to identify the malicious node, and energy efficiency, overhead and security features. That works didn't completely provide security features, energy efficient, less overhead. And also they dint deals with routing scheme**.** Wireless networks are vulnerable to various network attacks.

To cope with these security issues, trust-based routing schemes have emerged. Typically, trust routing schemes are mainly focused on detection of packet drop attacks, because this type of an attack is simple and obviously a malicious behavior. However, there are more advanced attacks, such as, false trust reporting or compromised attacks, where trust-based routing to defend these attacks is more difficult because of their ambiguous behavior.

2.1 Drawbacks

- ATR performance degradation occurs when the routing path's hop count is large.
- SPR shows the weakest performance among the three because most routes are blocked by malicious nodes.
- trust-based routing to defend these attacks is more difficult because of their ambiguous behavior.

3. PROPOSED SYSTEM

In order to ensure data transmission reliability even against such attacks, in this letter a centralized trust based secure routing scheme is proposed for wireless networks. AASR improves the routing performance by avoiding malicious nodes and effectively isolating false trust information offered by malicious nodes through a weight function. In addition, AASR considers nodal trust as well as directional trust to formulate a more reliable routing path.

A trust aware routing protocol is a routing protocol in which a node incorporates in the routing decision its opinion about the behaviour of a candidate router. This opinion is quantified and called trust metric. Trust metric should reflect how much a router is expected to behave, for example, forward a packet when it receives it from a previous node. Obtaining the trust metric is a problem by itself since it requires several operational tasks on observing nodes behaviour, exchanging nodes experience as well as modelling the acquired observations and exchanged knowledge to reflect nodes trust values.

Trust aware routing in WSN is important for both securing obtained information as well as protecting the network performance from degradation and network resources from un reasonable consumption. Most WSN applications carry and deliver very critical and secret information like military and health application. A WSN network infected by misbehaving nodes can misroute packets to wrong destinations leading to misinformation or do not forward packets to their destination leading to loss information .Such application can be very sensitive to these attacks. Having a trust aware routing protocol can protect data exchange, secure information delivery and maintain and protect the value of the communicated information.

Node misbehaviour can cause performance degradation as well. For example, non-forwarding attacks decrease the system throughput since packets will be retransmitted many times and they are not delivered. An infected WSN network can be partitioned into different parts that cannot communicate among each other due to non-forwarding attacks. This leads to the demand increasing the number of sensors or changing the node deployment to the demand of increasing the number of sensors changing the node deployment to return network connectivity.

This is very expensive however, can be avoided if a good secure routing solution is adopted. A trust aware routing framework for WSNs called sTARF to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information. This approach identifies malicious nodes that misuse "stolen" identities to misdirect packets by their low trustworthiness, thus helping nodes circumvent those attackers in their routing paths. It incorporates the trustworthiness of nodes into routing decisions allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. It significantly reduces negative impacts from these attackers.

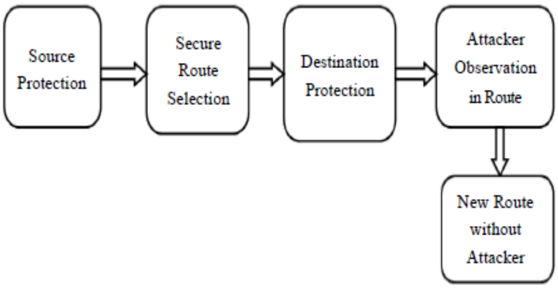

Figure 1: Block diagram of proposed mechanism.

Advantages:

- improves the routing performance
- avoiding malicious nodes
- effectively isolating false trust information offered by malicious nodes through a weight function
- Directional trust to formulate a more reliable routing path.

3.1 Modules:

1. Topology formation
2. Public Key & Session Key Distribution
3. AASR with Onion Routing
4. AASR Routing with Onion Routing & Trust

1. Topology Formation:

Constructing Project design in NS2 should takes place. Each node should send hello packets to its neighbour node which are in its communication range to update their topology.

2. Public Key & Session Key Distribution:

The key server is deployed. The predefined private keys are generated by the key server and the keys are distributed through the network between the wireless nodes.

3. Onion Routing:

It is a mechanism to provide private communications over a public network. The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node.

The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established.

4. AASR Routing & Trust Model:

- By using Trust model in *authenticated anonymous secure routing* (*AASR*), Data will be transmitted using Trusted Nodes.
- Untrusted nodes will not be considered during routing. This will reduce the delay occurred during RREQ and RREP phase of

AASR and also increase the network performance.

4. IMPLEMENTATION ENVIRONMENT

Network simulator2 is used as the simulation tool in this project. NS was chosen as the simulator because it has an open source code that can be modified and extended.

Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

5. CONCLUSIONS

In this letter, the CSR centralized trust-based routing scheme has been proposed to enhance reliable data transmission over networks that experience advanced attacks. CSR improves the routing performance by avoiding malicious nodes and effectively isolating false trust information offered by malicious nodes through a weight function.

In addition, CSR considers nodal trust as well as directional trust to formulate a more reliable routing path. Simulation results show that the CSR scheme provides an enhanced data routing performance for the range of interest compared to the ATR and SPR schemes in BHA and CBA attack scenarios.

REFERENCES

[1] S. Li, L. D. Xu, and S. Zhao, "The Internet of Things: A survey," Inf. Syst. Frontiers, vol. 17, no. 2, pp. 243-259, Apr. 2015.
[2] J.-H. Cho, A. Swami, and I.-R Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Commun. Surv. Tutor, vol. 14, no. 4, pp. 562-583, 2011.
[3] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Trans. Dependable Secure Comput., vol. 9, no. 2, pp. 184-197, Mar./Apr. 2012.
[4] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network," IEEE Sensors J. vol. 15, no. 12, pp. 6962-6972, Dec. 2015.
[5] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," IEEE Trans. Inf. Forensics Security., vol. 11, no. 9, pp. 2013-2027, Sep. 2016.
[6] X. Chen, J.-H Cho, and S. Zhu, "GlobalTrust: An Attack-Resilient Reputation System for Tactical Networks," in Proc. IEEE SECON 2014. Singapore, 2014, pp. 275-283.
[7] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941-954, Jul. 2010.
[8] M. Kurt and S. Peter, Algorithms and Data Structures: The Basic Toolbox. Springer, 2008. pp. 198-199. [5] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941-954, Jul. 2010.
[9] S. Zhu and Z. Ding, "Distributed cooperative localization of wireless sensor networks with convex hull constraint," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2150–2161, 2011
[10] S. Seo, J.-W. Kim, J.-D. Kim, and J.-M. Chung, "Reconfiguration time and complexity minimized trust-based clustering scheme for MANETs," EURASIP J Wirel Commun Netw, vol. 1, no. 155, pp. 1-7, 2017.