Review of Trust-based Security Models forPacket Routing in Wireless Sensor Networks

Sangeeta Rani[1] Dinesh Kumar[2] Vikram Singh[3]

[1]Research Scholar, Department of Computer Science & Engineering, University College of Engineering & Technology, Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India. sangeetathakral24@gmail.com

[2]Associate Professor, Department of Computer Science & Engineering, University College of Engineering & Technology, Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India.

[3]Professor, Department of Computer Science & Engineering, Chaudhary Devi Lal University, Sirsa, India, vikramsingh@cdlu.ac.in.

Abstract: In wireless sensor networks, routing deals with the delivery of data from a sensor node to the base station. Any attack on the routing mechanism can degrade or paralyze the operations of a wireless sensor network. Authentication and cryptographic solutions to thwart such attacks do not work, for these mechanisms are implemented using compromised nodes. Of lately, several trust-based schemes have been proposed to augment the security by excluding or including nodes in a route depending upon their computed trust values. Different trust mechanisms have been proposed to deal with different kinds of routing attacks. The present article reviews the current state of research in trust-based protocols for thwarting routing attacks in wireless sensor networks.

Keywords: Trust model, trust-based routing, trust-based secure routing, wireless sensor networks.

1. Introduction

This section introduces the concept of trust and its types, attacks on the routing mechanism, and the concept of securing routing.

1.1 Trust

Entrust® (2000) has defined the trust from viewpoint of users, the trust is inherent to every security system. Trust can assume different forms in different situations. The choice of the trust form to be used may be a personal choice or an organization policy. Usually, trust takes one of the two forms, namely, personal (direct trust) and third-party (indirect trust).

Direct trust can be described as a trust-based mutual relationship established between two individuals. This kind of trust is used to secure communications by two individuals from two separate organizations without any understanding ofthe key exchange. The indirect trust, on the other hand, does not mandate individuals to have a personal relationship for the secure exchange of information (Entrust® 2000).

1.2 Attacks against routing

Depending on the modi-operandi, the routing attacks can be classified intothe following two types (Velagaleti&Laxmi2008):

1. Resource consumption attacks target network resources like nodes' memory, energy, and bandwidth. These attacks may be realized by injecting extra data packets into the network.
2. Routing disruption attacks mainly affect the network routing process. These attacks may take several forms, e.g., the creation of a cyclic route, detouring the packets on a different route by faking control packets. These attacks may also lead to increased resource consumption. Blackhole attacks, greyhole attacks, and wormhole attacks are some examples.

Greyhole and blackhole differ by degree of severity and are perpetuated by feigning to show either a very short route or a high bandwidth link to the destination. Rushing attacks operate when identical control packets are rejected at the destination. Here control packets are disseminated rapidly thereby making the nodes reject the legitimate (duplicate) packets. These attacks work by replacing the old safe routes with spurious routes. In wormhole attacks two geographically distant nodes are made to 'think' that they are neighbors. This illusion is possibly given by a high-speed tunnel between such nodes. Such attacks are very difficult to detect and prevent.

1.3 Secure routing

Security in a wireless sensor network requires a combination of secure protocols for data aggregation and routing. To ensure that the data aggregation process culminated securely at the destination node/base station, the routing mechanism needs to be secure. Early routing protocols were devoid of any security measure for data aggregation. Later routing protocols, however, have started having inbuilt mechanisms to counter the attacks that compromise the route establishment. Most of such protocols exhibit a dynamic behavior in finding a route between source and destination nodes. Feiyi et al. (ud.) have proposed reactive secure routing protocols in which security code is invoked only when the network nodes stop working honestly.

2. Taxonomy of Trust Models

Trust models could be classified based on the location of storage of trust information. Accordingly, there would be three types of trust models, namely, centralized, distributed and hybrid trust models (Uma & Sundaram 2014). Taxonomy as proposed in Uma & Sundaram (2014) is shown in figure 1. In a centralized trust model, a single globally trusted server is used to compute the trust value in respect of every network node, whereas a distributed trust model is characterized by local computation of trust values of all other nodes in the network. The hybrid trust model assimilates the characteristics of both centralized and distributed trust models. The overhead cost of the distributed approach is higher in comparison tothe other two approaches.

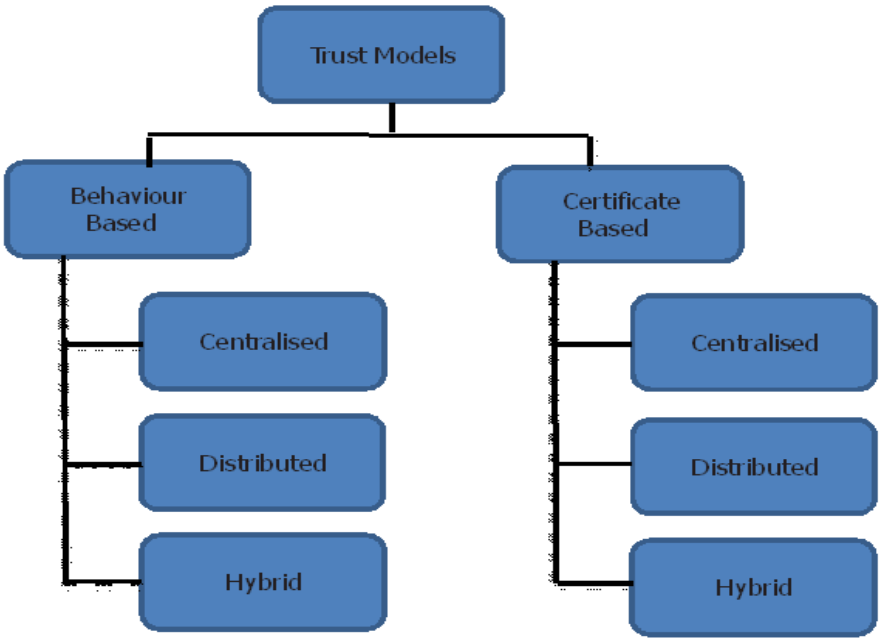

Figure 1. Classes of trust models [4].

In another classification, described in Uma & Sundaram (2014), trust models are bifurcated in the certificate-based and behavior-based models. In the former class, a centralized trusted authority issues the trust certificate to a target node, whereas, in the behavior-based trust model, the nodes' trust values are computed by an entity through continuous direct or indirect monitoring of the nodes.

In a wireless sensor network, trust plays a major role in detecting a node that is not behaving as expected (either faulty or maliciously). Trust judges the quality of node and their services. Also, it assists in the decision-making process such as data aggregation, routing and reconfiguring sensor nodes. Present communication focuses mainly on various trust models used in the wireless sensor network.

3. Trust-Based Routing Protocols

Of lately, secure routing in wireless sensor networks has assumed the center stage of network research endeavors. And, a host of trust-based security solutions of different flavors have been proposed for secure routing in WSN. The present section describes the contemporary research work in the field of trust-based routing protocols for wireless sensor networks (Ishmanov et al. 2015).

Probably the earliest trust-based model for sensor networks, wherein a watchdog technique was used in data gathering and event monitoring, was reported in Cho & Qu (2013). The watchdog mechanism identifies the nodes which do not forward packets. Zhou et al. (2015) have reported an extended watchdog mechanism that allows watching neighbour nodes' behaviour through direct observation, which in turn yield low processing overhead.

Guang et al (2009) and De-qin et al (2007) have proposed improved models of beta-based trust computation in wireless sensor networks. A lightweight trust management scheme has been proposed in Hai et al. (2010). Christened as 'The Retrust', it permits the detection of malicious nodes to improve the performance of sensor networks. The Lightweight Dependable Trust System (LDTS) of Hai et al. (2010) uses direct trust with feedback to strengthen decision making in a clustered WSN.

Mármol & Pérez(2008)proposed the bio-inspired trust and reputation model (BTRM) for wireless sensor networks. The model uses an ant colony reputation-based collaborative approach for selecting the most dependable node on the node-to-sink path. In Ozdemir(2008), a distributed reputation model has been proposed in the name of Reliable Data Aggregation and Transmission Protocol (RDAT). As the name suggests, the model ameliorates the reliability of data aggregation by a sensor node and its further transmission to the sink node. The trust management architecture (TMA) of Zhang (2010) is a certification-based trust model. It takes into account direct and indirect trust both and is claimed to reduce the processing overhead.

In Liu et al (2007), a resilient geographic routing (RGR) protocol has been developed to ensure trust-based secure routing. It uses a probabilistic multipath routing mechanism to thwart broadcast manipulation attacks. The trust management framework (TMF) of Zhang et al. (2010) is a hybrid of both certificate and behavior-based approaches and lessens the storage need as well as the processing and communication overheads. Authors in Shaikh et al. (2006) have proposed a distributed trust mechanism for the selection of the cluster head(s) dynamically computed as trusted. This prevents malicious nodes from assuming the role of the group head. Table 1.below has housed the summary of trust-based routing protocols wherein pros and cons and modi-oprandi of some such protocols.

Table 1. Trust-based Routing Protocol.

Protocol	**Trust evaluation method**	**Pros and cons**
LEACH based Trust Management Module (Song & Zhao 2008)	Constructs, maintains, and exchange trust information with adjacent sensor nodes. Combine direct trust and indirect trust.	Pros: Vulnerability to collusion attacks. Cons: Good defense against malicious nodes.
Fuzzy-based Method to Improve the Security (Raje& Sakhare2014)	A fuzzy-based trust model is used to calculate the trust of neighboring nodes to establish a reliable route.	Pros: Substantial increase in routing security. Cons: High energy consumption.
Routing Algorithm based on Trustworthy Core Tree (Wang et al. 2011)	Trust model is based on a trustworthy core tree that detects nodes exhibiting malicious behavior.	Pros: Effective detection of malicious nodes. Cons: Additional energy required for trustworthy core tree.
Trust-based Energy Efficient Routing protocol (Durrani et al. 2013)	Trust values of nodes are computed by the base station and used to establish multiple paths with differing degrees of security.	Pros: Thwarts wormhole and sinkhole attacks. Cons: No defense against internal attacks.

Cuckoo search based protocol (Senthil& Kannapiran2013)	Excludes all those routes whose trust values fall below a threshold. Multiple paths are considered for routing.	Pros: Less energy consumption and reduced end-to-end delay. Cons: Susceptible to internal and collusion attacks.
Trust-aware Routing Protocol with Multiple attributes (Sun & Li 2018)	Parameters considered for trusted routes are data, energy, communication, and recommended trust value.	Pros: Deals well with attacks originating from trusted nodes. Cons: Trust-aware cluster head selection is ignored.

4. Trust Models for Secure Packet Routing

Trust models described in contemporary literature have been reviewed and tabulated below in Table 2:

Table 2. Trust-based Secure Routing Protocol.

Protocol	**Method of security realization**	**Pros and cons**
Watermark technique-based method (Cheng et al. 2006)	The Watermark technique is employed to detect and calculate the packet loss at the destination node. The calculated packet loss rate is compared to an assumed normal packet loss rate. A node is considered malicious if its calculated packet loss rate comes out more than the normal packet loss rate.	Cons: Unrealistic assumption of normal packet loss rate may lead to wrong labeling of nodes.
Acknowledgment-based method (Altisen 2013)	Reception of a valid acknowledgment at the source node implies the successful delivery of data packet at the destination. Such an event increases the trust of a node in its neighboring node(s) involved in successful packet delivery.	Pros: Detection of genuine and malicious nodes is simple. Cons: Sending acknowledge for each packet is not energy efficient. Packet loss due to reasons other than maliciousness is not differentiated.
Random key pre-distribution scheme (Liu et al. 2016)	Attack detection involves routing data packets on various possible network paths. The presence of an attacker is assumed on the route if a packet is not delivered to the sink successfully.	Cons: The way the malicious nodes are detected and the type of attack considered are not specified in the learning component of the model.
Packet modification-based method (Johnson 1994)	Operates by checking the modification of the Dynamic Source Routing packet. This method works on the underlying assumption that data coming to a malicious node are modified and are forwarded to the colluding nodes.	Pros: Scheme of detection of the malicious node is very simple; Cons: Routing dependency and energy consumption overhead involved. Further, using only one criterion of attack to detect may be misleading at times.
Trust-based dynamic source routing (Pirzada et al. 2004).	Dynamic source routing has been adapted by changing its cost link to convey trust value of the node. Cost of the link is set to infinity for the node at the link-end. Performance evaluation report of the proposed routing algorithm suggests that it outperforms the GPSR and DSR in terms	Pros: Model takes in to account packet loss, throughput, and latency. Cons: Model does not consider energy consumption.

	of packet loss, throughput, and latency.	
Query-based routing (Naderi et al. 2015)	Firstly, sink node queries the network about the data packet till the time it reaches the source node. After receipt of the query, the source node broadcasts the data packets. Each subsequent node that gets the packet sends it to its neighbours.	Pros: Route detection method is quite general and is applicable to any routing protocol. Cons: Broadcast message causes message overhead and the energy consumption in routing is not considered.
Unsupervised genetic algorithm based method (Bankovićet al. 2011)	Unsupervised genetic algorithm is used to analyze the temporal and spatial inconsistencies in routing paths. An attack is assumed in case the inconsistency projection is over and above a given threshold.	Pros: The scheme provides accurate inference about attack. Cons: The scheme does not work well in the mobile environment.

5. Conclusion

In general, the trust-based routing protocols are established more efficiently vis a vis other routing mechanisms and yield a more secure routing of network traffic. Contemporary literature is rife with a plethora of trust-based routing protocols in general and trust-based secure routing protocols in particular. In trust-based models, the 'trust' is mathematically defined in terms of network parameters such as residual energy, packet signal strength, count of packets transmitted and received, count of control packets, etc. Trust value is computed for each of the alternative network paths between the source and sink nodes. Different secure routing models proposed in the literature differ in the expression for computing the trust value of network routes. This article has presented an overview of some relevant trust-based secure routing protocols.

References

1. Entrust® White Paper Version: 1.2 (2000). The Concept of Trust in Network Security, August 2000.
2. Velagaleti, N. R.&Laxmi, V. (2008). Attacks and countermeasures on routing protocols in wireless networks,*Graduate Theses and Dissertations*, 10586.
3. Feiyi W., Vetter, B., & Shyhtsun, F. W. (ud.). Secure Routing Protocols: Theory and Practice, *North Carolina State University* (ud.).
4. Uma R. V. & Sundaram, K. S. (2014). Review of Trust Models in Wireless Sensor Networks," *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 8, no. 2.
5. Ishmanov, F., Malik, A. S., Kim, S. W., & Begalov, B. (2015). Trust management system in wireless sensor networks: design considerations and research challenges,*Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130.
6. Cho, Y. &Qu, G. (2013). Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs,*International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 205920, 16 pages..
7. Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J., & Teo, J. C. M. (2015). Toward energy-efficient trust system through watchdog optimization for WSNs,*IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 613–625.
8. Guang, Y., Gui-sheng, Y., & Wu Y. (2009). Reputation Model based on behavior of sensor nodes in WSN, *Journal on Communication*, pp. 18-26.
9. De-qin, X., Jian-zhao, F., &Bo, Y. (2007). Reputation formal model for wireless sensor network" *Computer Science*, pp. 84-87.
10. Hai, T. H., Huh, E. N., & Jo, M. (2010). A lightweight intrusion detection framework for wireless sensor networks, *Wireless Communications and Mobile Computing*, vol. 10, no. 4, pp. 559– 572.

11. Mármol, F. G. &Pérez, G. M. (2008). Providing trust in wireless sensor networks uses a bio-inspired technique, *Journal on Communication*, pp.86-94.
12. Ozdemir, S. (2008). Functional reputation based reliable data aggregation and transmission for wireless sensor networks,*Computer Communications*, pp. 3941–3953.
13. Zhang, J., Shankaran, R., Orgun, M. A., Varadharajan, V., & Sattar, A. (2010). A Trust Management Architecture for Hierarchical Wireless Sensor Networks, in *35th Annual IEEE Conference on Local Computer Networks*, pp. 268-273.
14. Liu, K., Abu-Ghazaleh, N., &Kang, K. D. (2007). Location verification and trust management for resilient geographic routing, *Journal of Parallel and Distributed Computing*, 67, pp. 215 – 228.
15. Zhang, J., Shankaran, R., Orgun, M. A., Varadharajan, V., & Sattar, A. (2010). A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks, in *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 484 -492.
16. Shaikh, R.A., Jameel, H., Lee, S., Rajput, S., &Song, Y. J. (2006). Trust management problem in distributed wireless sensor networks, *12thIEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, pp. 411-414.
17. Song, F. & Zhao, B. (2008). Trust-Based LEACH Protocol for Wireless Sensor Networks,*2nd International Conference on Future Generation Communication and Networking*, vol. 1, pp. 202-207.
18. Raje, R. A.& Sakhare, A. V. (2014). Routing in Wireless Sensor Network Using Fuzzy Based Trust Model, in *International Conference on Communication Systems and Network Technologies* (CSNT). Bhopal, India. pp. 529-532.
19. Wang, J., Li, L.,& Chen, Z. (2011). A Routing Algorithm Based on Trustworthy Core Tree for WSN, in*IEEE/IFIP International Conference on Embedded & Ubiquitous Computing*, Hong Kong, China. pp. 763-770.
20. Durrani, N. M., Kafi, N., Shamsi, J., Haider, W., & Abbsi, A. M. (2013). Secure multi-hop routing protocols in Wireless Sensor Networks: Requirements, challenges and solutions, in *8thInternational Conference on Digital Information Management*, Islamabad, Pakistan. pp. 41-48.
21. Senthil, T.& Kannapiran, B. (2013). Ectmra: energy conserving trustworthy multipath routing algorithm based on cuckoo search algorithm. *Wireless Personal Communications*, vol. 94, no. 4, pp. 2239-2258.
22. Sun, B. &Li, D. (2018). A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs, *IEEE Access*, vol. 6, pp. 4725-4741.
23. Cheng, W., Liao, X., Shen, C., Li, S., &Peng, S. (2006). A trust-basedroutingframeworkinenergy-constrainedwirelesssensor networks,in *Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications (WASA '06)*, pp. 478–489, Xi'an, China.
24. Altisen,K.,Devismes,S., Jamet,R., &Lafourcade,P. (2013). SR3: secureresilientreputation-basedrouting,in*Proceedingsofthe 9thIEEEInternationalConferenceonDistributedComputingin Sensor Systems (DCoSS '13)*, Cambridge, Mass, USA.
25. Liu,Y., Dong,M., Ota,K., &Liu,A. (2016). ActiveTrust:secureand trustableroutinginwirelesssensornetworks,*IEEETransactionsonInformationForensicsandSecurity*,vol.11,no. 9,pp. 2013–2027.
26. Johnson,D. B. (1994). Routinginadhocnetworksofmobilehosts,"in *ProceedingsoftheWorkshoponMobileComputingSystemsand Applications*, pp. 158–163, Santa Cruz, California, USA.
27. Pirzada, A., Datta,A., &McDonald, C. (2004). Propagating trust inad-hocnetworksforreliable routing,"in*Proceedingsofthe International Workshop on Wireless Ad-Hoc Networks*, Oulu, Finland.
28. Naderi,O., Shahedi, M., &Mazinani,S. M. (2015). Atrust-based routingprotocolformitigationofsinkholeattacksinwireless sensor networks,*International Journal of Information and EducationTechnology*,vol.5,no.7,pp.520–526.

29. Banković, Z., Fraga,D., Vallejo,J.C., &Moya, J.M. (2011). Improving reputation systems for wireless sensor networks using genetic algorithms,in *Proceedings of the 13th Annual Genetic and Evolutionary Computation Conference (GECCO '11)*, pp. 1643– 1650,Dublin,Ireland.