Acknowledgement-Based Trust Framework for Wireless Sensor Networks

X. Anita[1], J. Martin Leo Manickam[2], and M.A. Bhagyaveni[1]

[1] Anna University, Chennai, India
anitaextee@yahoo.co.in
bhagya@annauniv.edu
[2] St. Joseph's College of Engineering, Chennai, India
josephmartin_74@yahoo.co.in

Abstract. Most of the existing trust-based routing schemes requires the support of promiscuous mode of operation and gathers large number of recommendations from the neighbors for trust derivation. In this paper, we propose a new Two-way Acknowledgement-based Trust framework with individual (2-ACKT-I) acknowledgements which calculates the direct trust using a link layer acknowledgement and a two-hop acknowledgement from a downstream neighbor. The simulation results demonstrate that 2-ACKT-I scheme significantly outperforms the conventional multihop routing schemes and promiscuous mode-based trust scheme in terms of packet delivery ratio and network lifetime.

Keywords: Trust, routing protocol, WSN, black hole, malicious attack.

1 Introduction

Wireless Sensor Networks (WSNs) consists of densely deployed tiny sensor nodes to monitor the real world environment by sensing, processing and communicating about the sensor field [1]. Due to the use of insecure communication channel, the WSNs are prone to varied types of attacks [2-5]. Several trust-based routing schemes are proposed in the literature to thwart the network layer attacks. Trust is the level of confidence in an entity and classified as direct and indirect trust [6]. The direct trust derivation requires promiscuous mode of operation which demands the sensor to be in the idle listening state till the next hop neighbor forwards the packet and hence, consume more energy. Moreover, the promiscuous mode of operation does not always provide sufficient evidence on the behavior of a monitored node. A monitored node may not be able to relay the packet due to the low quality of the wireless link. Alternatively, the indirect trust is derived based on the recommendations gathered from the neighbors. The large number of recommendations gathered from the neighbors increases the overhead and energy consumption in the network. Hence, the design objective of the proposed Two-way Acknowledgement based Trust (2-ACKT-I) framework with individual acknowledgements is to

V.V. Das and P.M. El-Kafrawy (Eds.): SPIT 2012, LNICST 117, pp. 34–40, 2014.

- To increase the network lifetime by avoiding the promiscuous mode of operation of sensors and thereby allowing the sensors to be in sleep mode as directed by the MAC,
- To reduce the memory requirement by representing the trust with lower number of bits, and
- To reduce the control overhead by minimizing the number of recommendations gathered in the network.

This paper is organized as follows: Section 2 describes the related work. Section 3 presents the proposed 2-ACKT-I protocol and performance analysis is presented in Section 4. The conclusions and future scope are followed in the Section 5.

2 Related Work

Many trust-based routing schemes proposed for WSNs uses either direct observation or recommendations or a combination of both to derive trust on its neighbors. Ganeriwal et al. proposed RFSN [7] scheme employs a watchdog mechanism and bayesian formulation to represent the trust based on the recommendations received from the neighbors. It will not cope with uncertain situation when the attacks are much more planned considering the weaknesses in different building blocks of the framework. Bourkerche et al. proposed ATRM [8] scheme uses the mobile agents in each node for trust management in clustered WSNs. It assumes the existence of a trusted authority to generate and launch mobile agents and so it is vulnerable to single point of failure. Most of the trust management schemes do not address the various resource constraint requirements of WSN but GTMS [9] proposed by Riaz Ahmed et al. has overcome some of these constraints. Each node calculates trust based on direct or indirect observations. Trust value is represented as an unsigned integer and saves memory space. The drawback of GTMS is that it demands high energy and more memory space for cluster heads (CHs). Moreover, it also assumes a trusted BS which is immune to security threats. Hosam A. Rahhal et al. proposed a TCLM [10] scheme for WSN and the trust are calculated by a cross-layer concept i.e by using ACKs from datalink layer and TCP layer. The trust value is represented in the range [0,1] as real numbers which requires more memory. The aforementioned trusted routing schemes uses promiscuous mode of operation for monitoring a neighboring node which incurs more energy in a resource constrained WSNs.

3 The 2-ACKT-I Routing Protocol

3.1 Assumptions

The 2-ACKT-I protocol is designed with the following assumptions:

- all nodes behave legitimately during route discovery stage,
- a peer-to-peer network with all SNs having unique identity,

- all nodes are homogenous with regard to storage capacity, processing speed and energy, and
- no collaborative attackers present.

The 2-ACKT-I protocol consists of the four components such as neighbor monitoring, trust computation, trust representation and 2-ACK routing protocol as shown in the Fig.1.

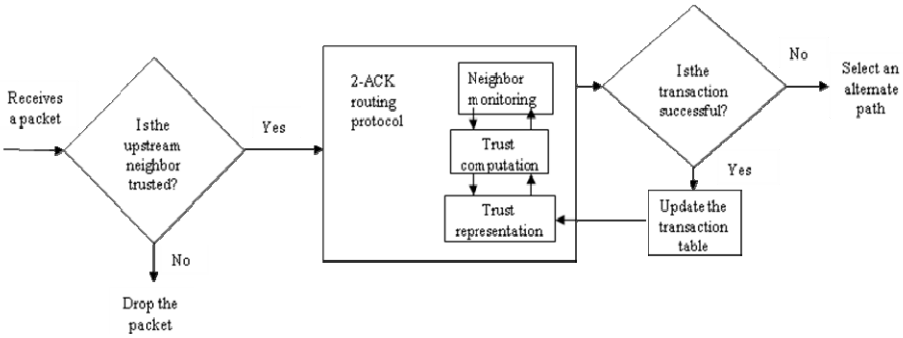

Fig. 1. Block diagram of 2-ACKT-I routing protocol

3.2 Neighbor Monitoring

The neighbor monitoring component in a trust-based routing scheme must ensure that the neighbor has successfully received the packet and it has forwarded the packet honestly to its neighbor by following the underlying routing protocol. Consider the topology shown in the Fig. 2.

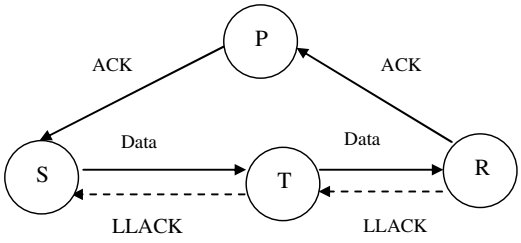

Fig. 2. Neighbor Monitoring

Let us assume that the subject (S) unicasts a data packet to its neighbor target (T). Being a legitimate node, target will forward the packet to its next hop sponsor (R) by following the underlying routing protocol. For accurate derivation of trust, the subject must ensure the occurrence of the following two events:

(1) Target has successfully received the packet sent by it, and

(2) Target has forwarded the packet to its downstream neighbor R faithfully following the protocol.

In 2-ACKT scheme, the occurrence of event (1) is ensured by using the link layer acknowledgement (LLACK) generated from the IEEE 802.15.4 MAC protocol.

The occurrence of event (2) is ensured by unicasting a two-hop ACK to the subject through the alternate path R-P-S as shown in the Fig. 2 where P is the third party neighbor. The alternate path is determined during the route discovery stage by exploiting the dense nature of the sensor network as discussed in the section 3.4. The subject on receiving a LLACK from the target and subsequently an acknowledgement from sponsor through the alternate path will consider that transaction as successful one else it is considered to be failed.

3.3 Trust Computation and Representation

The observed successful and failed transactions are stored in the transaction table. The fields in the transaction table of the subject are as follows:

<*node id, number of successful transactions* (T_s), *number of failed transactions* (T_f), *trust level* (T_L)>

where *node id* is the address of the neighbor namely target, *number of successful transactions* is incremented by 1 when individual acknowledgement is received, *number of failed transactions* is incremented by 1 when it has not received the ACK in a given timeout, and *trust level* can take an integer value from 0 to 7 as shown in the Fig. 3. The trust value is computed based on the observed number of successful and failed transaction entries in the transaction table as given by

$$T_V = \left(\frac{T_s + \varepsilon}{T_s + T_f} \right) * 100 \tag{1}$$

where ε is a constant. The computed T_V lies in the range [0,100] and it is not directly stored in the transaction table as it consumes more memory. It is mapped to one of the possible trust level (T_L) as shown in the Fig. 3. T_L can take an integer value which lies in the range [0,7] and requires memory space of 3 bits. A target is considered to be trusted when $T_L > 3$. Any request or response from an untrusted target will not be considered during route discovery and packet forwarding stages.

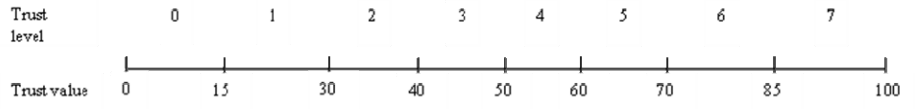

Fig. 3. Trust Representation

3.4 2-ACK Routing Protocol

When a SN desires to report an event to the BS for which a valid route is not found, it initiates a route discovery process by broadcasting a route request (RREQ) to its neighbor. The RREQ contains the following fields:

<source_address, source_seq_#, broadcast_id, destination_seq_#, hop_cnt, upstream_neighbor_address>

The pair *<source_address, broadcast_id>* uniquely identifies a RREQ. *broadcast_id* is incremented whenever the source issues a new RREQ. *upstream_neighbor_address* is the address of the neighbor from which it receives the RREQ. On receiving a RREQ packet from a neighbor, the intermediate SN verifies whether the packet is received from a trusted neighbor by checking the transaction table. If the neighbor SN is found to be trustworthy, each neighbor either satisfies the RREQ by sending a route reply (RREP) packet to the source or rebroadcasts the RREQ to its own neighbor after incrementing the *hop_cnt* and updating the *upstream_neighbor_address*. Subject address is derived from the *upstream_neighbor_address* in the received RREQ. A node may receive multiple copies of same RREQ packet from various neighbors. If a node receives redundant RREQ packet i.e with same *broadcast_id* and *source_address* as in the processed RREQ, then it does not rebroadcast the packet but it verifies the *upstream_neighbor_address* in the received RREQ. If the *upstream_neighbor_address* is same, then the node records the address of the neighbor from which it has received the redundant copy of RREQ to establish the alternate path to the subject. This neighbor is referred as third party neighbor as it relays RREQ with same *broadcast_id*, *source_address* and *upstream_neighbor _address* as in already processed RREQ. Once the RREQ reaches the BS or an intermediate SN with a fresh enough route, the BS or an intermediate SN responds by unicasting an RREP packet back to the neighbor from which it first received the RREQ. Each route table entry contains the following information:

<destination address, next hop, number of hops, destination sequence number, active neighbors for this route, third party neighbors for this route, expiration time for the route table entry>.

Each SN maintains a route table entry for each destination of interest.

4 Results and Discussion

The performance of 2-ACKT-I protocol is studied using the ns-2 simulator. The malicious nodes manifest black hole attack [2]. We took a simulation area of 300 X 300 m, with six hundred nodes placed in random. The transmission range is 45 m. The IEEE 802.15.4 is the MAC layer protocol used to evaluate the performance of the proposed trust model under attack conditions. We have also implemented the promiscuous mode-based trust (PMT-AODV) scheme in AODV [11] routing protocol. The 2-ACKT-I, PMT-AODV and AODV protocols are tested against exactly the same scenario and connection pattern. In AODV, the discovered route to the BS may consist of malicious nodes. As a result, the packet loss in AODV is 61.9 percent higher than 2-ACKT-I protocol as shown in Fig. 4(a). The malicious nodes are effectively identified and eliminated in the discovered route and hence results in lower packet loss in 2-ACKT-I and PMT-AODV protocols. This has a positive effect

on the packet delivery ratio (PDR) of the 2-ACKT-I and PMT-AODV protocols as shown in the Fig. 4(b). 2-ACKT-I routing protocol augments the PDR of the AODV routing protocol by up to 28.57 percent. The performance of 2-ACKT-I and PMT-AODV are almost the same. In 2-ACKT-I routing protocol, the sponsor sends ACK to the subject through the third party for every data packet received from the target. As a result, the control overhead of 2-ACKT-I is 45.44 percent higher than AODV protocol. In PMT-AODV, all the neighboring sensor nodes overhear the control packets as well as the data packets to compute trust. As a result, the control overhead is 16.07 percent higher than 2-ACKT-I as shown in Fig. 4(c). The simulation is performed with an initial energy of 0.5 joules to calculate the network lifetime. The higher energy consumption for trust evaluation of 2-ACKT-I and PMT-AODV protocol results in lower network lifetime of 3.79 percent and 5.34 percent respectively over AODV routing protocol as shown in Fig. 4(d). The lower overhead and non-promiscuous mode of operation for trust evaluation in 2-ACKT-I protocol keeps the network lifetime 1.61 percent higher than that of PMT-AODV.

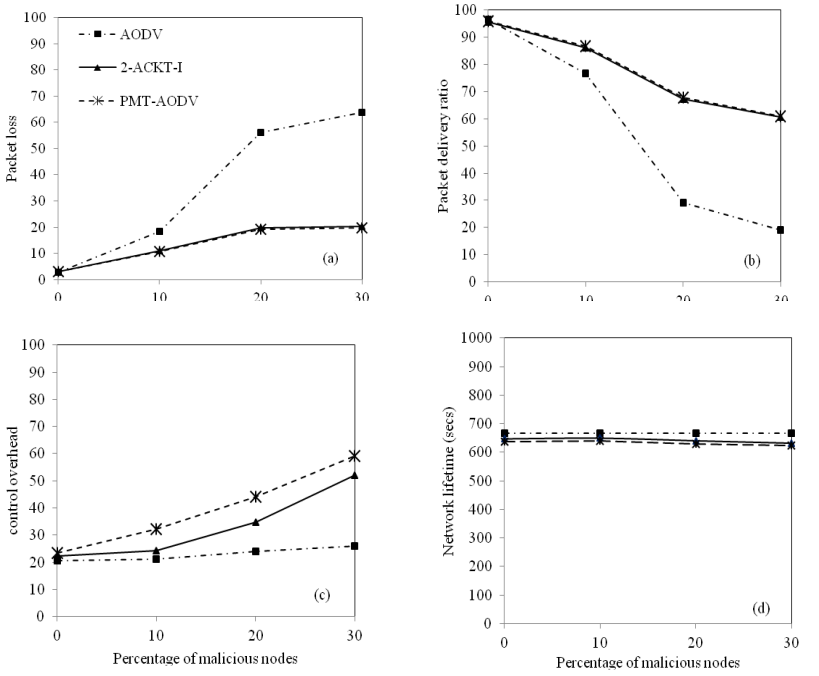

Fig. 4. Performance Comparison of 2-ACKT-I, PMT-AODV and AODV routing protocols

5 Conclusion

Security is an important problem that can significantly degrade the performance of resource constrained WSNs. In this paper, we have proposed a new 2-ACKT-I

framework for trust evaluation in WSNs. The simulation results show that the proposed protocol has better performance than the conventional multihop and trust-based routing protocols in terms of packet delivery ratio, control overhead and network lifetime. In this paper, the malicious attacks are manifested by individual sensor nodes. However, there exists a much wider spectrum of security threats involving collaborative attackers. Hence, we plan to design a comprehensive trust-based security solution that thwarts collaborative attackers in a resource constrained WSNs.

References

1. Chen, X., Makki, K., Yen, K., Pissinou, N.: Sensor Network Security: A Survey. IEEE Communications Surveys & Tutorials 11(2), 52–73 (2009)
2. Wang, Y., Attebury, G., Ramamurthy, B.: A Survey of Security Issues in Wireless Sensor Networks. IEEE Communication Surveys and Tutorials 8(2), 2–23 (2006)
3. Yu, Y., Li, K., Zhou, W., Li, P.: Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures. Journal of Network and Computer Applications, 867–880 (2012)
4. Hoffman, K., Zage, D., Rotaru, C.N.: A Survey of Attack and Defense Techniques for Reputation Systems. ACM Computing Surveys 42(1), 1–31 (2009)
5. Karlof, C., Wagner, D.: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Journal on Elsevier's Ad Hoc Networks, Special Issue on Sensor Network Applications and Protocols 1(2-3), 293–315 (2003)
6. Momani, M., Challa, S., Alhmouz, R.: Can We Trust Trusted Nodes in Wireless Sensor Networks? In: Proceedings of the International Conference on Computer and Communication Engineering, pp. 1227–1232 (2008)
7. Ganeriwal, S., Srivatsava, M.B.: Reputation-Based Framework for High Integrity Sensor Networks. In: Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, p. 66 (2004)
8. Boukerche, A., Li, X., EL-Khatib, K.: Trust-Based Security for Wireless Ad Hoc and Sensor Networks. Computer Comm. 30, 2413–2427 (2007)
9. Ahmed, R., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., Song, Y.-J.: Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems 20(11), 1698–1712 (2009)
10. Rahhali, H.A., Ali, I.A., Shaheen, S.I.: A Novel Trust-Based Cross-Layer Model for Wireless Sensor Networks. In: 28th National Radio Science Conference, vol. C5, pp. 1–10 (2011)
11. Perkin, C.E., Royer, E.M.: Ad Hoc On Demand Distance Vector Routing. In: Second IEEE Workshop on Mobile Computing, Systems and Applications, pp. 90–100 (1999)