Trust Based Energy Preserving Routing Protocol in Multi-hop WSN

Saima Raza[1(✉)], Waleej Haider[1], Nouman M. Durrani[2], Nadeem Kafi Khan[2], and Mohammad Asad Abbasi[1]

[1] Sir Syed University of Engineering and Technology, Karachi, Pakistan
saimarzaidi@gmail.com
[2] FAST NUCES, Karachi, Pakistan

Abstract. Wireless Sensor Networks (WSN) are widely used in many sensitive applications, where human deployment is almost impossible. Due to resource constraints, the network and hence the forwarded information is open for attacks. Hence, it is desirable to ensure source to sink privacy in order to maximize the network lifetime. In this paper we studied security threats and energy constraints while deploying WSN nodes. Moreover, we propose a Trust Based Secure and Energy Preserving Routing Protocol (TEPP), in multi-hop WSN. The proposed solution monitors reputation and trust worthiness of nodes and maintains a history of interaction between nodes to identify secure and trust worthy path. The effectiveness of our proposed protocol has been experimentally verified against various attacks. At the end future research directions have been highlighted.

Keywords: WSN · Trust-based · Energy efficient · Secure routing

1 Introduction

Wireless sensor network (WSN) is a network of small and smart computing devices for establishing reliable, scalable and resilient network of sensing and forwarding nodes. WSN are mainly deployed in many applications such as industrial power control, environmental monitoring, medical instrumentation and homeland security, where human intervention is difficult. In such networks, it is required to maximize network lifetime and strengthen source to sink privacy, by finding trustworthy, secure and energy-efficient route discovery and forwarding mechanisms.

As, these networks deal in sensitive data and are opened due to limited resources, it is important to make them secure against various types of attacks such as spoofing, selective forwarding, sinkhole attacks, wormholes, traffic analysis node replication and attacks against privacy. Moreover, the attackers can easily demolish the whole network by capturing the network nodes or by attacking the routing protocol. Even few computational resources are enough to shoot up fake messages, operate routing messages, attack the routing protocols and disrupt the normal operation of the network. Even more, arbitrary behavior may be induced by corrupting the intermediate nodes or planting an internal attacker into the network. Considering all these realities, the deployment of a secure routing protocol becomes a primary task; however, designing of such secure

A. Bouajjani and H. Fauconnier (Eds.): NETYS 2015, LNCS 9466, pp. 518–523, 2015.
DOI: 10.1007/978-3-319-26850-7_42

routing protocols are not easy. An important factor in this regard is energy-aware trustworthy secure routing, which is significant in ensuring smooth operation of WSNs [1]. Careful management of the network is also desired, as processing required for secure routing and communication is distributed over the nodes itself. Providing security in such networks is extremely important and challenging.

Generally, WSN system threats fall in three categories with reference to security considerations: confidentiality, availability and integrity [2]. Many researchers suggested trust management system to help in selection of trust worthy peer of same behavioral pattern [3–6]. Some of trust metrics depends upon recommendation system but our proposed algorithm doesn't support recommendation system as they may suffer from badmouthing attack. According to Xiong et al. [7] reputation is a key factor which adds value to trust certificate whereas Sen et al. [8] proposed that reputation and rating framework has several lacunas due to dishonest parties and great numbers of variables for assessing trust.

Providing an accredited vocabulary, string of trust and delegated permissions as designed in by Freudenthal et al. [9] in Role-based access control model. Several researcher proposed to integrate processing modules with in WSN for observing and calculating different parameters for selection of optimal path [10, 11]. However these protocol may magnify traffic in WSN as regular broadcast of message from BS and sensors nodes require more computing power as two computing components run on nodes. Considering the limited computational and energy constraints, in this paper we have presented a trust based routing scheme called "Trust Based Energy Preserving multihop Routing Protocol (TEPP)" for secure data transmission in WSNs in Sect. 2, followed by the performance and evaluation of our proposed protocol in Sect. 3. Afterwards conclusion is drawn with future research directions.

2 Proposed Solution

The protocol called as TEPP comprises of three phases: Neighbor Identifying Phase, *Cluster Head Selection phase and Data Sharing Phase.* It provides a secure information sharing path and controls malicious nodes by providing a mechanism of authentication and trust calculation of each node. The network consists nodes, cluster Heads and the BS. BS has a centralized control and helps to reduce the Bandwidth and computation requirements of network. Our proposed routing protocol uses Modified Closest pair-wise keys pre-distribution scheme for secure communication between two nodes [12]. All server nodes have their master keys provided by setup server and for every pair of node (IDS, IDR), a pair-wise key KS, R = PRF KR (S) is generated where PRF is pseudo random function. New sensor node has predefined keys for all sensor nodes in its transmission range. Hash Message Authentication Code (HMAC) is applied to provide message integrity and to verify sender authentication. TEPP Phases are described as under:

Neighbor Identifying Phase: In Neighbor Discovery Phase, node initiates zero messages using "Modified dynamic, zero-message broadcast encryption scheme based on Secure Multiparty Computation" [13] to discover its neighbors with in transmission range. This broadcast message has two blocks cipher block and header block. Header block has message id and list of several receiver nodes where message id is unique. Cipher block is encrypted using one-time key (OTK) which is calculated: OTK = Combine t, n (K_1, K_2, …. K_n) where Ki = H(ID message, ID RNode, Key RNode, ID SNode) where RNode is recipient node, SNode is source node and ciphers block is composed of (ID SNode, Nonce SNode) information. Interested Nodes sends reply message with in time out as follows:

$$\mathrm{ID_{RNode}} \rightarrow \mathrm{ID_{SNode}} = \mathrm{K_{R,S}}[(\mathrm{Nonce_{RNode}} \parallel \mathrm{ID_{RNode}}) \parallel (\mathrm{ID_{SNode}} \parallel \mathrm{Nonce_{SNode}})]$$

Sender Node decrypts this acceptance message using its private key and adds nodes in its neighbor list. Sharing of data within a cluster requires minimum level of energy.

Cluster Head Selection Phase: In proposed algorithm Cluster Heads are decided by applying LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm [13] under surveillance of BS. CH behaves as an intermediate channel between sensor nodes and base station, and maintains communication history table CHT shown in Table 1, of nodes located in respective cluster and calculates a threshold value of each node using formula: $T_{Th} = f(MI) + TR + EN + FP$; where, TR is data transmission range of node, EN indicates energy of node; FP is number of times sensor node participated in communication, *f* (MI) function of integrity is calculated on basis of frequency of errors, link failures, Message verification techniques thus CH and BS help a sensor node to choose best data transferring node among several alternatives. Initially, nodes have no information about their respective neighbors. To initiate trust calculation, flooding mechanism is introduced and CHT is created. During and after neighbor detection phase all sensor nodes update about malicious nodes to their respective CH, which share this information to all other nodes within and outside the Clusters. After CH is decided, it detects its surrounding CH by broadcasting a zero message encrypted using OTK after getting response message it updates CH neighbor list. BS after receiving information about CH and their neighbor calculates multipath and share secret pair keys with all CH.

Data Sharing Phase: When node wants to transmit data, it uses distance vector algorithm to find all available route towards destination and CH helps sending node in

Table 1. Communication history table (CHT)

Source	Destination	f (MI)	TR (Meters)	EN (Volts)	FP	Threshold value
A	B	01.40	60	3.2	4	68.6
B	E	01.10	50	2.2	8	61.3
B	D	00.75	45	3.5	3	52.25
E	F	01.00	56	2.4	7	66.4
D	F	01.20	60	2.4	7	70.6
F	C	01.35	45	3.1	5	54.4

deciding best among multiple route options i.e. When a node “A” wants to send information to destination node “C”, it finds several alternatives path using modified distance vector algorithm.

i. A– –>B– –>E– –>F– –>C   ii. A – –>B– –>D – –>F– –>C

Than Cluster Head using “CHT” works in reverse order i.e. it will forward the data on nodes with high **threshold** (trust value) for the destination node “C” which is node “F” in this sample case. We can express this path selection and data forwarding on the following expression:

$$\begin{aligned} A - - > B &: HMAC\left(K_{A,B}, Data, ID_A, ID_B\right) \\ &= H[(ID_A \parallel (Ku \oplus opad)) \parallel H[((Ku \oplus ipad) \parallel Data \parallel ID_B)]] \end{aligned}$$

Since only trustworthy nodes are selected in the data forwarding process, hence the impact of malicious nodes is decreased. Moreover, the energy is conserved as only trusted nodes are involved in the data forwarding process. In the next section we discuss performance of our proposed protocol against various types of attacks and their impact on the packet delivery or packet drop.

3 Performance and Evaluation

The proposed protocol provides a mechanism which keeps track of malicious behavior within network to combat unfair acts by any node and sensed data is transferred through node with high threshold value with combination of energy aware mechanism. OMNeT++ has been used to simulate the performance of our proposed protocol. Initially a test bed of 100 nodes with an average calculated threshold 54.6 was evaluated against 15 % malicious nodes involved in different types of attacks such as wormhole, selective forwarding, and de-synchronization attacks. The proposed protocol was evaluated against ATSR, GPSR and TARF routing protocols. Experimentally, it has been found that only 14 % of the packets were dropped. Further, when the numbers of malicious nodes were increased randomly to 40 % of 2000 nodes, the packet drop ratio was observed to be stable. As shown in Fig. 1, less than 33 % packets were unable to reach the destination node. In the same case, major packet drop was observed for ATSR, GPSR and TARF. It shows that the protocol is exceptionally stable under large number of attacks. Proposed TEPP compared with TARF, TEESR, Trusted GPSR protocols and analyzed that it performs better in providing defensive measures against De-Synchronization, Selective Forwarding, Wormholes attacks. Table 2 highlights the impact of different attacks on threshold value of individual node calculated using TEPP. It shows that three to four time occurrence of attack decreases threshold value of nodes thus degrading trustworthiness of that node. Also, it has been

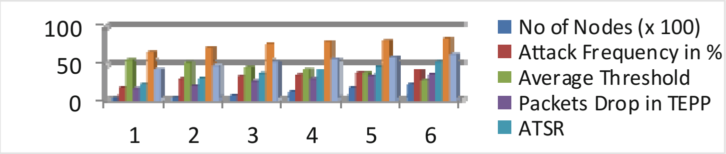

Fig. 1. Effect of security attacks on packet delivery

Table 2. Impact of different attacks on threshold value of node calculated using TEPP

Nodes	De-Synchronization			Selective Forwarding			Wormholes		
	A_F	T_H	I_F	A_F	T_H	I_F	A_F	T_H	I_F
A	5	54.6	Medium	2	58.00	Low	4	53.24	Medium
B	4	51.00	Medium	6	45.23	High	5	50.66	Medium
C	4	45.00	Medium	4	47.80	Medium	7	40.23	High
D	4	45.4	Medium	4	48.50	Medium	3	55.27	Low
E	2	60.6	Low	6	43.24	High	3	52.00	Low
F	7	34.4	High	4	40.23	Medium	8	36.12	High

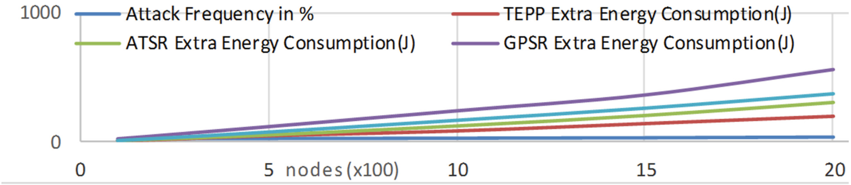

Fig. 2. Extra energy consumption (in J/×100 nodes) due to packet drop

found that for the same network when compared with other routing protocols such as TARF, ATSR and GPSR protocols also shown Fig. 2.

4 Conclusion

Due to various security challenges in WSNs, we have presented a Trust Based Energy Preserving multihop Routing Protocol that not only tends to mitigate major security risks but also provides an energy efficient data forwarding mechanism. Performance in terms of packet drop and extra-energy consumption was evaluated against various secure and energy efficient protocols. Processing power required for head nodes to maintain history and trust calculation of each node and to combat energy exhaustion required in movement of nodes between clusters is left for future research.

References

1. Stajano, F.: Security issues in ubiquitous computing. In: Nakashima, H., Aghajan, H., Augusto, J.C. (eds.) Handbook of Ambient Intelligence and Smart Environments, pp. 281–314. Springer, Heidelberg (2010)
2. Durrani, N.M., et al.: Secure multi-hop routing protocols in wireless sensor networks: requirements, challenges and solutions. In: 8th IEEE ICDIM (2013)
3. Carullo, G., et al.: FeelTrust: providing trustworthy communications in Ubiquitous Mobile environment. In: 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA). IEEE (2013)
4. Pirzada, A.A., McDonald, C.: Trusted greedy perimeter stateless routing. In: 15th IEEE International Conference on Networks, ICON 2007. IEEE (2007)
5. Bao, F., et al.: Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Netw. Serv. Manag. **9**(2), 169–183 (2012)
6. Li, X., Lyu, M.R., Liu, J.: A trust model based routing protocol for secure adhoc networks. In: IEEE Proceedings on Aerospace Conference, vol. 2 (2004)
7. Xiong, L., Liu, L.: PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowl. Data Eng. **16**(7), 843–857 (2004)
8. Sen, S., Sajja, N.: Robustness of reputation-based trust: boolean case. In: Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, Bologna, Italy, 15–19 July 2002
9. Freudenthal, E., Pesin, T., Port, L., Keenan, E., Karamcheti, V.: dRBAC: distributed role-based access control for dynamic coalition environments. In: Proceedings of the 22nd ICDCS 2002. IEEE Computer Society, July 2002
10. Zhan, G., Shi, W., Deng, J.: TARF: A trust-aware routing framework for wireless sensor networks. In: Sá Silva, J., Krishnamachari, B., Boavida, F. (eds.) EWSN 2010. LNCS, vol. 5970, pp. 65–80. Springer, Heidelberg (2010)
11. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc. In: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom). ACM Press, pp. 255–265 (2000)
12. Liu, D., Ning, P.: Location-based pairwise key establishments for static sensor networks. In: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. ACM (2003)
13. Soodkhah, M., Mohammadi, A., Bafghi, G.: A dynamic, zero-message broadcast encryption scheme based on secure multiparty computation. In: 9th ISC (2012)