ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(32), DOI: 10.17485/ijst/2015/v8i32/87509 , November 2015* ISSN (Online) : 0974-5645

Theoretical Analysis of Trust-based Routing Schemes for Wireless Sensor Networks

X. Anita[1] and A. Kumaravel[2]*

[1]Department of Information Technology,Jerusalem College of Engineering, Chennai - 600100, Tamil Nadu, India
[2]Department of Information Technology, Bharath University, Chennai - 600073, Tamil Nadu, India; kumaravel.cse@bharathuniv.ac.in

Abstract

WSNs comprises of densely deployed tiny sensor devices deployed in sensitive applications. The security systems designed does not consider the constraints of sensor nodes. Trust of the network depends on packet forwarding behavior of the neighbor. The communication overhead depends on the number of packets transmitted for trust computation. The memory consumption depends on the size of the trust tables used for trust computation. In this paper, we have presented the communication overhead and memory consumption of the existing trust based routing schemes.

1. Introduction

Trust depend on the level of confidence of a sensor node and it can be classified as direct and indirect trust[2]. Trust a node could be computed based on direct or indirect observation or combination of both. In direct observation, node A transmits a packet to its neighbor B and checks the packet forwarding activity of the neighbor B. If the node B has forwarded the packet to its next hop downstream neighbor, then node A considers that transaction as successful and increases the trust of that node. For indirect observation, node A calculates trust of B by gathering recommendations.

2. Related Works

In GTMS[3], the trust model was based on two different topology i.e., intragroup and intergroup topology[1]. Distributed trust management approach was used in intragroup topology whereas in intergroup topology, centralized trust management approach was used. Each node computes the trust of its based on direct or indirect observation. For direct observation, the node uses promiscuous mode of operation i.e., overhearing the transmission of neighbor[2]. When there is no direct interaction, then the node collect recommendations from the neighbors. In distributed trust management, each node in a group maintains the trust of all its group members and so when a node wants to collect recommendation of another node in its same group, then it send peer recommendation request and receiver peer response from all its group members. In centralized trust management, the BS maintains the trust of all the CHs in the network[3]. When a CH wants to collect recommendation about a CH in another group, then it will send one recommendation request to the BS and receive one recommendation response. The trust is represented in 1 byte in the range between 0 and 100 i.e., as integer[4].

* *Author for correspondence*

In LDTS[4], the centralized trust management approach was used in both intragroup and intergroup topology. Each node computes the trust of its based on direct and indirect observation. The promiscuous mode of operation was used for direct observation. The CH maintains trust of all its cluster members and BS maintains trust of all CHs in the network. When a node wants to collect recommendation of another node in its same group, then it sends one recommendation request to its CH and receives one recommendation response. Similarly, when a CH wants to collect recommendation of a CH in another group then it sends one recommendation request to BS and receives one response. The trust value was represented in 4 bits in the range of 0 to 10[5].

In 2-ACKT[5], a distributed trust management approach was used and the trust computation was based on direct observation. For direct monitoring, node A monitors the packet forwarding behavior of its downstream neighbor B by a two hop acknowledgement sent by the two hop downstream neighbor of A in an alternate path identified by exploring the dense nature of WSNs[6].

3. Theoritical Analysis

3.1 Communication overhead

LDTS

In LDTS, when a node from ith group wants to communicate with the BS through its CH, the node sends a maximum of one CH feedback request and in turn receives a maximum of one response[7]. Therefore, the communication overhead for the interaction between a node and its CH is,

$$C_{LDTS(N-CH)} = 2 \quad (1)$$

When a CH of ith group wants to communicate with CH of jth group, it sends one sink feedback request and receives one feedback from the sink. Then the communication overhead for the interaction between two adjacent CHs is $C_{LDTS(CH\text{-}CH)} = 2$.

When a CH of ith group wants to collect feedback from its cluster members, it will send a maximum of σ feedback request and receives σ responses, where σ is the average size of the group. Therefore, the communication overhead for collecting feedback by all CHs is $C_{LDTS(CH-N)} = 2\sigma$. The communication overhead incurred by all CHs to collect the feedback from their cluster members is obtained by multiplying $C_{LDTS(CH-N)}$ by $\frac{N}{\sigma}$, where $\frac{N}{\sigma}$ is the average number of CHs,

$$C_{LDTS(CH)} = 2\sigma\left(\frac{N}{\sigma}\right) \quad (2)$$

When the BS wants to collect feedback from the CH, it will send a maximum of $\frac{N}{\sigma}$ feedback request and receives $\frac{N}{\sigma}$ responses, where $\frac{N}{\sigma}$ is the average number of CHs. Therefore, the communication overhead for collecting feedback is,

$$C_{LDTS(BS)} = 2\left(\frac{N}{\sigma}\right) \quad (3)$$

As the sink is considered to be trusted, if a node present in the ith group wants to communicate with the BS in h hops, then the communication overhead is obtained by multiplying $C_{LDTS(CH-CH)}$ by h - 2 and adding the product to Equation 6 as given by,

$$C_{LDTS(N-BS)} = 2 + 2(h-2) = 2(1+(h-2)) \quad (4)$$

If all the $'N'$ number of SNs want to communicate with the BS, then the total communication overhead is obtained by multiplying Equation 4 by N and adding the Equation 2 and Equation 3,

$$C_{LDTS} = 2N(1+(h-2)) + 2\sigma\left(\frac{N}{\sigma}\right) + 2\left(\frac{N}{\sigma}\right) \quad (5)$$

GTMS

As described in [19], the communication overhead of GTMS [12] protocol can be derived as

$$C_{GTMS} = 2N(\delta + h - 4) \quad (6)$$

2-ACKT

As described in [19], the communication overhead is

$$C_{2-ACKT} = 2N(h-1) \quad (7)$$

3.2 Memory Consumption

LDTS

In LDTS, SN maintained a transaction table to monitor and store the trust level of their neighbors. The fields in the transaction table and its memory size are

shown in the Table 5[8]. The node id occupied 2 bytes, number of successful transactions and number of failed transactions occupied 2 bytes each, trust level and peer recommendation required 4 bits each[9]. Therefore, the memory required to store a record in the transaction table that represented the trust relationship with a neighbor was 7 bytes. The total size of the transaction table that represented the trust relationship between an SN and all its neighbors was

$$M_{LDTS(SN)} = 7(\sigma - 1) \text{ bytes} \quad (8)$$

where σ is the average number of SNs in a cluster.

In addition to trust table present in the SN, the CH maintains another trust table to store the feedback from all cluster members. Therefore, the total memory requirement of CH

$$M_{LDTS(CH)} = 7\left(\frac{N}{\sigma} - 1\right) + 0.5(\sigma - 1)^2 \quad (9)$$

where $\frac{N}{\sigma}$ is the average number of CHs in a network.

The total memory required for a network that consists of N number of nodes and $\left(\frac{N}{\sigma}\right)$ number of CHs is determined by adding the products obtained by multiplying Equation 25 by N and Equation 26 by $\left(\frac{N}{\sigma}\right)$ as given by

$$M_{LDTS} = 7N(\sigma - 1) + \left(\frac{N}{\sigma}\right)\left[7\left(\frac{N}{\sigma} - 1\right) + 0.5(\sigma - 1)^2\right] \quad (10)$$

Assuming $\sigma = n$ the Equation 26 is rewritten as

$$M_{LDTS} = 7N(n - 1) + \left(\frac{N}{n}\right)\left[7\left(\frac{N}{n} - 1\right) + 0.5(n - 1)^2\right] \quad (11)$$

GTMS

As described in [19], the memory consumption of GTMS [12] protocol can be derived as

$$M_{GTMS} = (4 + 4n)\left\{N(\delta - 1) + \left(\frac{N}{\delta}\right)\left(\frac{N}{\delta} + \delta - 2\right)\right\} \text{ bytes}$$

2-ACKT

As described in [19], the total memory requirement for the entire network which consists of N number of sensors is

$$M_{2\text{-}ACKT} = 6.375nN \text{ bytes} \quad (13)$$

where n is the average number of neighbors for each SN.

4. Conclusions

Security is an important problem that can significantly degrade the performance of resource constrained WSNs. The communication overhead and memory consumption incurred should be minimal in a resource constrained WSNs. In this work, we have presented the theoretical analysis of 2-ACKT, GTMS and LDTS routing protocols based on communication overhead and memory consumption.

5. References

1. Kimio T, Natarajan G, Hideki A, Taichi K, Nanao K. Higher involvement of subtelomere regions for chromosome rearrangements in leukemia and lymphoma and in irradiated leukemic cell line. Indian Journal of Science and Technology. 2012 April; 5(1): 1801–1811.
2. Cunningham CH. A laboratory guide in virology. 6th edn. Minnesota: Burgess Publication Company; 1973.
3. Sathishkumar E, Varatharajan M. Microbiology of Indian desert. In: Sen DN, editor. Ecology and Vegetation of Indian Desert. India: Agro Botanical Publishers; 1990. p. 83–105.
4. Varatharajan M, Rao BS, Anjaria KB, Unny VKP, Thyagarajan S. Radiotoxicity of sulfur-35. Proceedings of 10th NSRP; India. 1993. p. 257–8.
5. 01 Jan 2015. Available from: http://www.indjst.org/index.php/vision
6. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communication Magazine. 2002; 40(8):102–14.
7. Krishnamoorthy P, Jayalakshmi T. Preparation, characterization and synthesis of silver nanoparticles by using phyllanthusniruri for the antimicrobial activity and cytotoxic effects. Journal of Chemical and Pharmaceutical Research. 2012; 4(11):4783–94. ISSN: 0975 – 7384.
8. Momani M, Challa S, Alhmouz R. Can we trust trusted nodes in wireless sensor networks? Proceedings of the International Conference on Computer and Communication Engineering; 2008. p. 1227–32.
9. Madhubala V, Subhashree AR, Shanthi B. Serum carbohydrate deficient transferrin as a sensitive marker in diagnosing alcohol abuse: A case - Control study. Journal of Clinical and Diagnostic Research. 2013; 7(2):197–200. ISSN: 0973-709X.
10. Ahmed R, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y-J. Group-based trust management scheme for clustered wire-

less sensor networks. IEEE Transactions on Parallel and Distributed Systems; 2009 Nov; 20(11):1698–712.
11. Khanaa V, Thooyamani KP, Saravanan T. Simulation of an all optical full adder using optical switch. Indian Journal of Science and Technology. 2013; 6(S6):4733–6. ISSN: 0974-6846.
12. Anita X, Martin Leo Manickam J, Bhagyaveni MA. Two-way acknowledgment-based trust framework for wireless sensor network. International Journal of Distributed Sensor Networks. 2013; 952905:14.
13. Nagarajan C, Madheswaran M. Stability analysis of series parallel resonant converter with fuzzy logic controller using state space techniques. Electric Power Components and Systems. 2011; 39(8):780–93. ISSN: 1532-5008.
14. Li X, Zhou F, Du J. LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Transactions on Information Forensic and Security; 2013; 8(6):924–35.
15. Bhat V. A close-up on obturators using magnets: Part I - Magnets in dentistry. Journal of Indian Prosthodontist Society. 2005; 5(3):114–8. ISSN: 0972-4052.