International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 03, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

Secure and Trustable Routing in WSN for End to End Communication

Maniyar Aasif Mashak[1] | Prof.V.V.Dakhode[2]

[1,2] Department of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Maharashtra, India.

To Cite this Article
Maniyar Aasif Mashak and Prof.V.V.Dakhode, "Secure and Trustable Routing in WSN for End to End Communication", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 03, 2017, pp. 19-24.

ABSTRACT

In WSNs, end-to-end data communication security is required to combine data from source to destination. Combined data are transmitted in a path exist of connected links. All previous end to end routing protocols propose solutions in which each n every link uses a pair wise shared key to protect data. In this paper, we propose a novel design of secure end to end data communication. We give a newly published group key pre distribution scheme in this design, such that there is a unique group key, called path key, to protect data transmitted in the whole routing path. Specifically, instead of using several pair wise shared keys to repeatedly perform encryption and decryption over every link, our proposed scheme uses a unique source to destination path key to protect data transmitted over the path.

Our proposed protocol can authenticate sensors to establish the path and to establish the path key. The main advantage using our protocol is to reduce the time needed to process data by middle sensors. Moreover, our proposed authentication scheme has complexity O(n), where n is the number of sensors in a communication path, which is several from all authentication schemes till now, which are one-to-one authentications with complexity O(n2). The security of the protocol is computationally secure. Active Trust can importantly improve the data route success probability and ability opposite black hole attacks and can optimize network lifetime.

KEYWORDS: *Black Hole Attack, Network Lifetime, Security, Trust, Wireless Sensor Networks.*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have been deployed in several applications to combine information from human body, battle fields, smart power grids, Interstate highways, etc. Sensors are subjected by their physical drawback on hardware, storage space, computational power, etc. Developing capability solutions to protect information in sensor networks is a challenging task. User authentication and key create are two fundamental security functions in most secure communications. The user authentication enables communication entities to authenticate characteristics of their communication partners. After users being successfully authenticated, a key create enables a secret session key to be shared among nodes involved in communication such that all exchange information can be protected using shared key provided between nodes. Traditional communications are one-to-one type of communications which demand only two communication entities. Most existing user authentication schemes combine only two entities, one is the prover and the other one is the verifier. The verifier interacts with the prover to validate the identity of the prover. However, communication has been moved to many-to-many communications currently, also called group communications. Traditional user authentication which

authenticates one user at one time is no longer suitable for a group communication which involves more users. Recently, a new type of authentication, called group authentication, is proposed which can be used to determine is there all users belong to the same group or not. The group authentication is very efficient since it can authenticate all members at one time. However, the group authentication can only be used as a pre-processing of authentication of the user since if there are non-members, group authentication cannot determine who non-members are. Additional one-to-one user authentications are needed to identify non-members.

II. REVIEW OF LITERATURE SURVEY

Joint Optimization of Lifetime Transport Delay under Reliability Constraint Wireless Sensor Networks: This paper first presents an investigation method to meet requirements of a sensing application through trade offs between energy consumption (lifetime) and source-to sink transport delay under reliability rule wireless sensor networks.

Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory. In this paper, we first formulate the price competition model of SOS where the SOS dynamically increase and decrease their service prices periodically according to the several collected services from entities. A game based services price decision (GSPD) model which depicts the process of price resolution is proposed in this paper. In GSPD model, entities game with other entities under the rule of "survival of the fittest" and calculate payoffs according to their own payoff matrix, which leads to a Pareto-optimal equilibrium point.

Energy and Memory Efficient Clone Detection in Wireless Sensor Networks. In this paper, we propose an energy-efficient location-aware clone detection protocol in densely deployed Wireless Sensor Networks, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location data of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks.

An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration. In this paper, we advancingly explored the authentication as well as trust reputation calculation and management of CSPs SNPs, which are two very critical and barely explored issues with respect to CC and WSNs integration. Further, we proposed a novel ATRCM system for CC-WSN integration.

Towards Energy-Efficient Trust System through Watchdog Optimization for WSNs. In this paper, we reveal the inefficient use of watchdog technique in existing trust systems, and there by propose a suite of optimization methods to minimize the energy cost of watchdog usage while keeping the systems security in a sufficient level. Our contributions consist of theoretical analyses practical algorithms which can efficiently effectively schedule watchdog tasks depending on sensor nodes locations and target nodes trustworthiness.

III. SYSTEM ARCHITECTURE

In this paper, we propose a novel design of secure end-to-end data communication. We acquire a newly published group key pre-distribution scheme in our design such that there is a unique group key, called path key, to protect data transmitted in entire path. Specifically, instead of using multiple pair wise shared keys to repeatedly perform encryption and decryption over every link, our proposed scheme utilize a unique end to- end path key to protect data transmitted over the path. Our protocol can authenticate sensors to establish a routing path and to establish a path key. The important advantage of our protocol is to reduce the time needed to process data by intermediate sensors. In this paper we propose security and trust routing through an active detection route protocol. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection path, it will attack these routes and, in so doing, be exposed. In this way, the attackers behavior and location, as well as nodal trust, can be obtained and utilized to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs. In our proposed system we create group key for security. When received node they have not group key then this node cant received packet and also this node cant transfer packet.

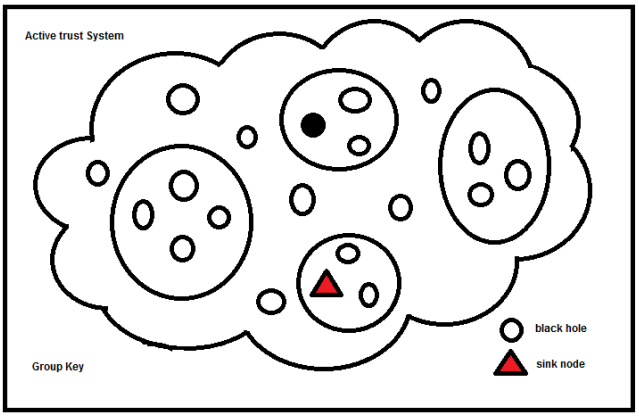

Fig.1: *System architecture of End to end secure communication*

IV. SOFTWARE REQUIREMENT SPECIFICATION

Proposed design is planned to implement above requirement using following system configuration.

Operating System- Windows7,XP

Coding Language – Java

Tool – Ecipse Luna

Functional Requirements

1. Design overlapped network simulator
2. Data collection in wireless sensor
3. Network cluster formation
4. Determination of sink node or Base station in cluster
5. Multiple path selection for multipath routing
6. Shared node detection and recovery.
7. Active source routing for energy efficiency.
8. Network aware routing.
9. Throughput maximization
10. Reduce packet delay ratio by cluster based routing.

Non-Functional Requirements

The non-functional requirements of the system are explained below as performance Requirements and design constraints.

Performance requirements

1. Response Time

The system shall respond to any request in few seconds
from the time of the request submittal. The system shall
be allowed to take more time when doing large processing jobs.

Software Quality Attributes

1.Usability

The system should be user friendly and self-explanatory. Since all users are familiar with the general usage of computers, no specific training should be required to operate the system. Apart from this, the system should be highly Reliable, Flexible, Robust, and easily Testable.

2.Accuracy

Since we will give the priority to the accuracy of the software, the performance of the Music Recommender will be based on its accuracy on recommendations.

3.Failure handling

System components may fail independently of others. Therefore, system components must be built so they can handle failure of other components they depend on.

4. Openness

The system should be extensible to guarantee that it is useful for a reasonable period of time.

5. Usability

The software will be embedded in a website. It should be scalable designed to be easily adopted by a system.

6. Reliability

The system should have accurate results and fast responses to user are changing habits.

V. MATHEMATICAL MODEL

Let us consider S as a system for Energy hole evolution for data analysis in WSN

Assume that node j is in the small region of Ax with the width of ε. Denote x as the distance between Ax and the sink, and θ as the angle formed by Ax and the sink. If each node generates one data packet per round, the average data amount sent by j in a round at S0 is,

$$P_j^{(0)} = \begin{cases} (z_1+1)+\frac{z_1(1+z_1)r}{2x} & z_2 \ (\ z_2+1 \ )r \ \varepsilon\theta\rho \ , \\ \frac{1}{2}(z_2+2)\varepsilon^2\theta\rho+\frac{1}{2} & \text{otherwise} \end{cases}$$

Where,

$z_1 = \llcorner (R-x)/r \lrcorner$ and $z_2 = \llcorner (R-\varepsilon)/r \lrcorner$

Since node j is in the small region of A_x, its traffic load can be calculated as the average traffic load in Ax according to our analytic model. Therefore, we first calculate the average traffic load in A_x. ε is the width of Ax and θ denotes the angle formed by Ax and the sink; thus, we can obtain the number of nodes in Ax As these nodes receive and forward the data from the upstream regions, the number of sensor nodes in the upstream regionsA_{x+ir},

$$N_{A_{x+ir}} = \begin{cases} (x+ir)\epsilon\theta\rho | 0 < i \le z_1, \\ \left(\frac{\varepsilon}{2}+ir\right)\varepsilon\theta\rho | 0 < i \le z_2 \end{cases}$$

Where,

$z_1 = \llcorner (R-x)/r \lrcorner$ and $z_2 = \llcorner (R-\varepsilon)/r \lrcorner$

Since each node only generates a data packet per round, the number of data packets equals to the number of the involved nodes. Thus, the number of data packets sent by Ax is,

$D_{A_x}=N_{A_x}+N_{A_{x+r}}+\ldots\ldots\ldots\ldots+N_{A_{x+zr}}$

We have the average traffic load of Ax as $\frac{D_{A_x}}{N_{A_x}}$ .Since the traffic load of the node j approximately equals the average traffic load of the sensor nodes in Ax, the traffic load of the node j at S_0 should be $P_j^{(0)}=\frac{D_{A_x}}{N_{A_x}}$.

With some simple calculation, we have $P_j^{(0)}$.

S= {……

INPUT:

Identify the inputs

F= {f1, f2, f3 …..,fn| 'F' as set of functions to execute commands.}

I= {i1, i2, i3…|'I' sets of inputs to the function set}

O= {o1, o2, o3….|'O' Set of outputs from the function sets}

S = {I, F, O}

I = {Number of sensor node, sink node, nearest nodes, data packet size, transmission rate}

O = {Reduced energy hole evolution for data acquisition.}

F = {Functions implemented to get the output}

Shortest Path Problem:-

Input: a weighted graph

G= (V, E)

The edges can be directed or not

Sometimes, we allow negative edge weights

VI. ALGORITHM

Active Detection Routing Protocol Algorithm

Determination of energy time and boundary of energy hole Algorithm

1: Initialization

2: For each neighbor node A_n do

3: Let A_n accessTime=current_time

4: End for

5: For each node that generates a detection packet, such as node A, do

6: Construct packet P, and do value assignment for ω and ϖ

7: Select B as the next hop which B meets access time is the minimum and nearer the sink

//B is the node that is the longest time undetected and nearer the sink

8:Send packet P to node B

9: End for

10: For each node that receives detection packet, such as node B, do

11: let p. ω= p. ω -1, ϖ =p. ϖ -1

12: If ϖ=0 then

13: Construct feedback packet q, and do value assignment for each part

14: Send feedback packet q to the source

15: End if

16: if p. ω ≠ 0 then

17: detection routing continue

18: End if

19: End for

20: For each node that receives feedback packet q, such as node C, do

21: If q.detection is not itself then

22: send q to the source node

23: End if

24: End for

Data Routing Protocol Algorithm

1: For each node that generate or receives a data packet, such as node A, do

2:select B as the next hop such that B has never been selected in this data routing process, has the largest trust and is nearer the sink

3:If A finds such node, for instance, node B

4: send data packet P to node B

5: If node B is the sink then

6: this data routing procession is completed

7: End if

8:Else

9: Send failure feedback to the upper node, such as node C

10: End if

11: End for

12: For each node that receives failure feedbacks, such as node B, do

13: Repeat step 2 to step 10

14: End for

VII. RESULT ANALYSIS

The probability of successful routing of the Active Trust scheme for different BLAs. In the experiment, the black hole attack refers to the malicious attack in which all data that attempt to pass by are dropped. However, the Denial-of- Service Attack refers to the attack in which data are dropped intermittently, thus making it difficult to resist this attack. The select forward attack is one of the most intelligent attacks and can drop data selectively [6]. It can be seen from below charts that the Active Trust scheme has positive effects on the different impacts of BLAs.

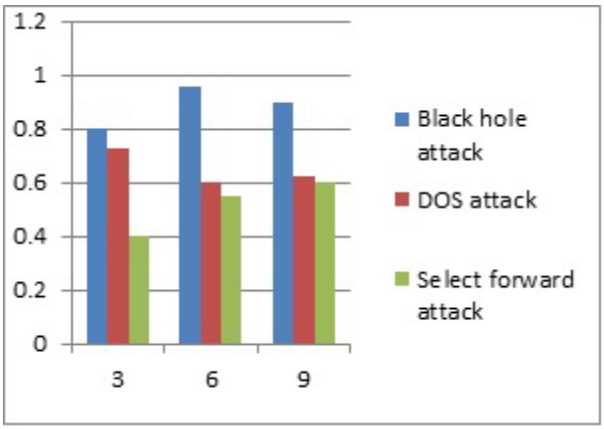

Fig. Probability of succesful routing for different BLAs.

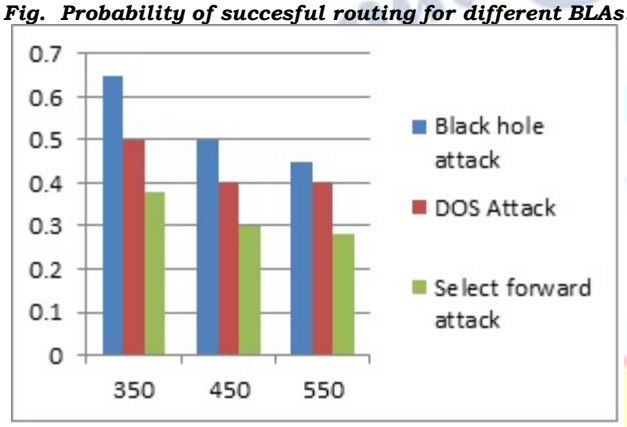

Fig. Probability of succesful routing for different numbers of black holes for different BLAs.

Result Table

Parameter	Value
Threshold Distance (d_0) (m)	90
Sensing range r_s (m)	30
E_{elec} (nJ/bit)	60
Initial Energy	1.0
e_{amp} (pJ/bit/m^4)	0.0120
e_{fs} (pJ/bit/m^2)	20

VIII. COMPARISON WITH SIMILAR SYSTEM

Existing system and disadvantages:-

A black hole attack (BLA) is one of the most typical attacks and works as follows. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs. There is much research on black hole attacks. However, the current trust-based route strategies face some challenging issues. (1) The core of a trust route lies in obtaining trust. However, obtaining the trust of a node is very difficult, and how it can be done is still unclear. (2) Energy efficiency. Because energy is very limited in WSNs, in most research, the trust acquisition and diffusion have high energy consumption, which seriously affects the network lifetime. (3) Security. Because it is difficult to locate malicious nodes, the security route is still a challenging issue.

Disadvantages of existing system

1. Energy Consumption Problem
2. Not provide Security during Packet transmission
3. The network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions.

Proposed system advantages:

1. The ActiveTrust scheme is the first routing scheme that uses active detection routing to address Block hole attacks (BLA).
2. The ActiveTrust route protocol has better energy efficiency.
3. The ActiveTrust scheme has better security performance.

IX. CONCLUSION

In this paper, we have proposed security and trustable routing scheme based on active detection, and it has the following outstanding properties: (1) High successful routing probability, security and scalability. The ActiveTrust scheme can fast detect the nodal trust and then avoid dubious nodes to quickly achieve a nearly 100 percent successful routing probability.

(2) High energy efficiency. The ActiveTrust scheme fully uses residue energy to construct several number of detection routes. The theoretical analysis and experimental results have shown that our scheme improves the successful routing possibility by more than 3 times, up to 10 times in some cases. Another, our scheme improves both the energy efficiency and the network security performance. It has crucial significance for wireless sensor network security. In this paper .we are using group key establishment for security with properties k-secure, key confidentiality and key independence.

REFERENCES

[1] M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

[2] X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016.

[3] Z. Zheng, A. Liu, L. Cai, et al."Energy and Memory Efficient Clone Detection in Wireless Sensor Networks,"IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp.1130-1143,2016.

[4] C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

[5] P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

[6] LeinHarn and Ching-Fang Hsu," Predistribution Scheme for Establishing Group Keys in Wireless Sensor Networks", IEEE Sensors Journal, vol. 15, no. 9, September 2015

[7] SushmitaRuj, AmiyaNayak and Ivan Stojmenovic," Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications", IEEE Transactions on Computers,2012.

[8] LeinHarn and JianRen, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", IEEE Transactions on wireless communication, vol. 10, no. 7, July 2011

[9] WenjunGu, NeelanjanaDutta, SriramChellappan, and XiaoleBai," Providing End-to-End Secure Communications in Wireless Sensor Networks", IEEE Transactions on Network and Service Management, VOL. 8, NO. 3, September 2011

[10] H. Liang and C. Wang, "An energy efficient dynamic key management scheme based on polynomial and cluster in wireless sensor netwoks,", J. Converg. Inf. Technol., vol. 6, no. 5, pp. 321–328, 2011.