ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Survey on Secure and Trustable Routing In Wireless Sensor Network for End To End Communication

Prof Vina M. Lomte, Kavita V. Dubey

HOD, RMD Sinhgad School of Engineering. Pune, India

Student, RMD Sinhgad School of Engineering. Pune, India

ABSTRACT: In wireless sensor networks, the secure end-to-end data communication is needed 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 link uses a pairwise 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 our design, such that there is a unique group key, called path key, to protect data transmitted in the entire routing path. Specifically, instead of using several pairwise shared keys to repeatedly perform encryption and decryption over every link, our proposed scheme uses a unique end-to-end path key to protect data transmitted over the path. Our 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 existing authentication schemes which are one-to-one authentications with complexity *O(n2)*. The security of the protocol is computationally secure. ActiveTrust can importantly improve the data route success probability and ability oppositeblack hole attacks and can optimize network lifetime.

KEYWORDS: Black Hole Attack, Network Lifetime, Security, Trust, Wireless Sensor Networks, Secure communications, group keys,authentication, secret sharing.

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 communication entities such that all exchange information can be protected using this shared key. Traditional communications are one-to-one type of communications which demand only two communication entities. Most existing user authentication schemescombine 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 whether 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 user authentication 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

II. REVIEW OF LITERATURE

1. Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks.

Refer Points-

This paper first presents an investigation method to meet requirements of a sensing application through trade-offs between the energy consumption (lifetime) and source-to-sink transport delay under reliability rule wireless sensor networks.

Advantages- Reduced node energy consumption.
Disadvantages-Transmission of packet takes more times.

2. Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory.

Refer Points-

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 **g**ame based **s**ervices **p**rice **d**ecision (GSPD) model which depicts the process of price resolution is proposed in this paper. In the 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.

Advantages-Some entities will die because of competition failure in the game, and some entities can gain competitive advantage in the competition and occupy the dominant position.

Disadvantages-While the service price of the entity is too low; other entities have no desire to interact with them, which leads to the entity being at a disadvantage to competition.

3. Energy and Memory Efficient Clone Detection in Wireless Sensor Networks.

Refer Points-
In this paper, we propose an energy-efficient location-aware clone detection protocol in densely deployed WSNs, 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.

Advantages-
Location information by distributing the traffic load all over WSNs, such that the energy consumption and emory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.
Disadvantages- In this paper not using different mobility pattern under various network scenarios.

4. An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration.

Refer Points-
In this paper, we advancingly explored the authentication as well as trust and reputation calculation and management of CSPs and 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Advantages-Improve their trust and reputation values faster than the honest participants or counter the effects of possible negative feedbacks.

Disadvantages-In that paper not providing Security during packet transmission.

5. towards Energy-Efficient Trust System through Watchdog Optimization for WSNs.

Refer Points-
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 system's security in a sufficient level. Our contributions consist of theoretical analyses and practical algorithms which can efficiently and effectively schedule watchdog tasks depending on sensor nodes' locations and target nodes' trustworthiness.

Advantages-Ultimategoal is to reduce the energy cost induced by watchdog tasks asmuch as possible, while keeping trust accuracy and robustness
in a sufficient level.

Disadvantages-In this paper disadvantage is that minimum throughput.

III. SYSTEM OVERVIEW

Software Requirement Specification
Software Requirements

Operating System -	LINUX	
Tool	-	Network Simulator-2
Front End	-	O TCL (Object Oriented Tool Command Language)

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
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
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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Apart from this, the system should be highly Reliable, Flexible, Robust, and easily Testable.

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.

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.

Usability

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

Reliability

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

Safety Requirements

No harm is expected from the use of the product either to the OS or any data that resides on the client system.

Product Security Requirements

The product is protected from un-authorized users from using it. The system allows only authenticated users to work on the application. The users of the system are network users (Sender & Receiver).

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 *S*0 is,

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

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. $\varepsilon$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 theupstream regions, the number of sensor nodes in the upstreamregionsA_{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,

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

We have the average traffic load of Ax as $\frac{D_{Ax}}{N_{Ax}}$.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_0should be $P_j^{(0)}=\frac{D_{Ax}}{N_{Ax}}$. With some simplecalculation, we have$P_j^{(0)}$.

S= {……

INPUT:

Identify the inputs

F= {f_1, f_2, f_3 ……,f_n| 'F' as set of functions to execute commands.}

I= {i_1, i_2, i_3…|'I' sets of inputs to the function set}

O= {o_1, o_2, o_3….|'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}

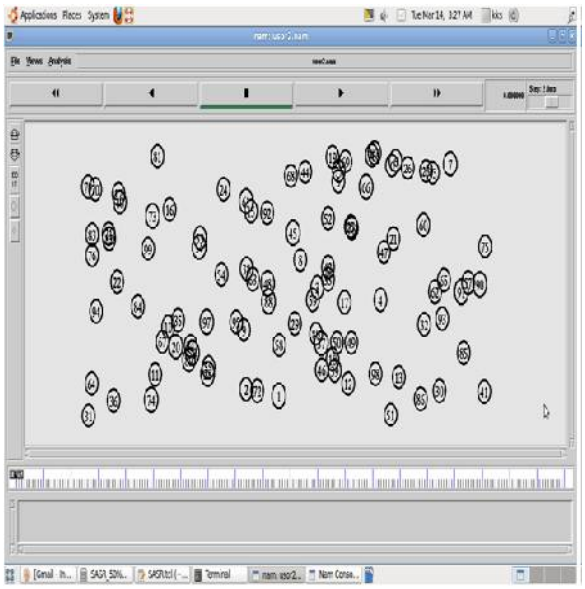
O = {Reduced energy hole evolution for data acquisition.}

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

Output: The path between two given nodes U and v that minimizes the total weight (or cost, length) Sometimes, we want to compute all-pair shortest paths Sometimes; we want to compute shortest paths from U to all other nodes.

Implementation Status



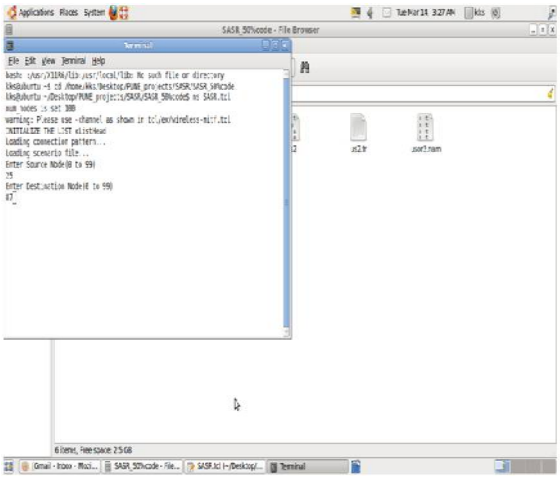
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

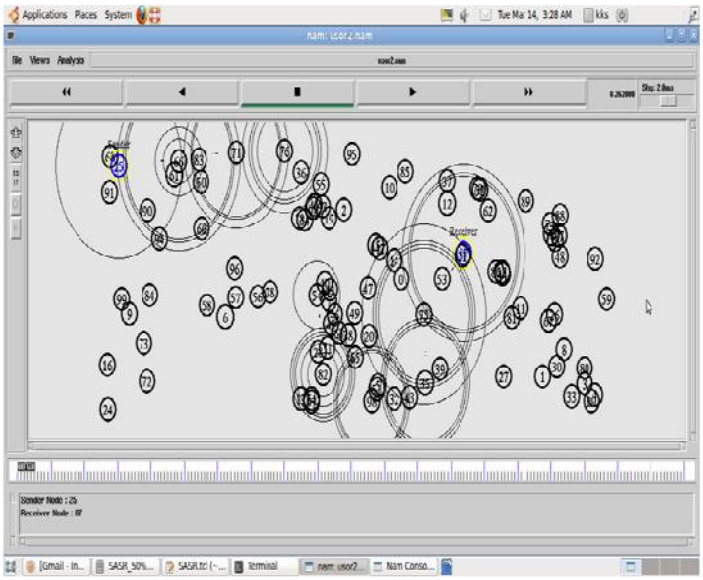
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017





IV. COMPARISON WITH SIMILAR SYSTEM

Existing System

A black hole attack (BLA) is one of the most typical attacks and works asfollows. 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

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.

In this paper, we propose a novel design of secure end-to-end data communication. We acquire a newly publishedgroup key pre-distribution scheme in our design suchthat there is a unique group key, called *path key*, to protectdata transmitted in entire path. Specifically, instead of usingmultiple pairwise shared keys to repeatedly perform encryptionand decryption over every link, our proposed scheme utilize aunique end-to-end path key to protect data transmitted overthe path. Our protocol can authenticate sensors to establish arouting path and to establish a path key. The important advantage ofour protocol is to reduce the time needed to process data byintermediate sensors.In this paper we propose security and trust routing through an active detection route *protocol.* The most significant difference between ActiveTrust 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 attacker's 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 can't received packet and also this node can't transfer packet.

Advantages of Proposed System:

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.

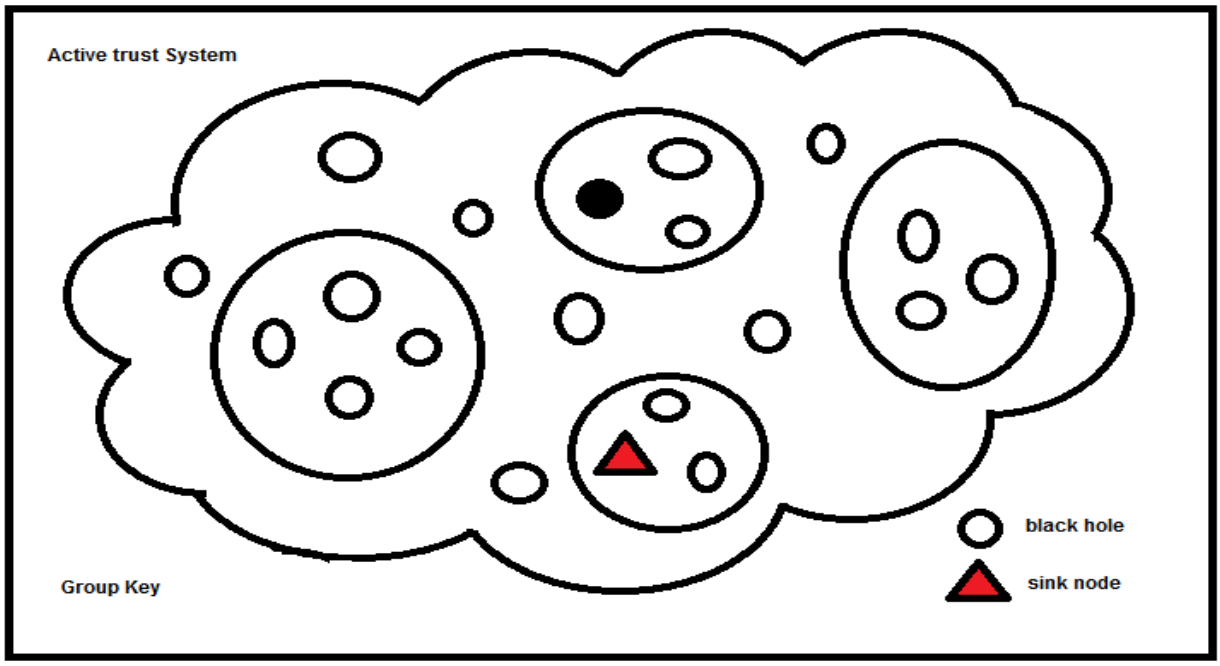


Fig. Proposed System

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

V. SYSTEM ANALYSIS

Performance Measures Used

The probability of successful routing of the ActiveTrust 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 [35, 36], 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 Figs. 34 and 35 that the ActiveTrust scheme has positive effects on the different impacts of BLAs.

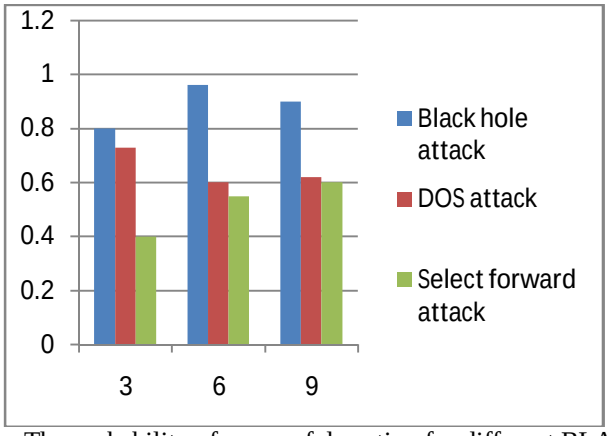


Fig. The probability of successful routing for different BLAs.

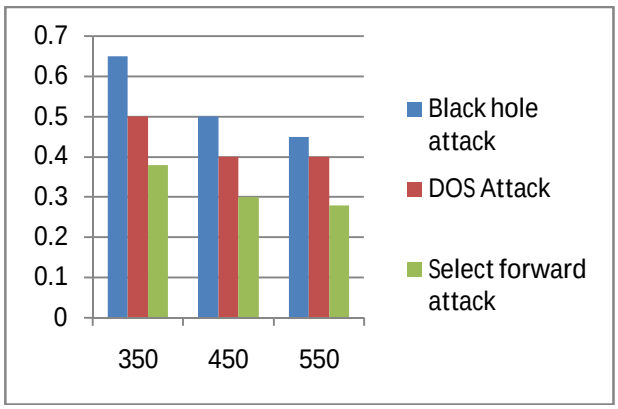


Fig. The probability of successful routing under different numbers of black holes for different BLAs.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Result Table

Table 1 network parameters

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

Efficiency Calculation

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,

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

VI. CONCLUSION

In this paper, we have proposed a novel security and trust 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% 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 propertiesk-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. S. He, J. Chen, X. Li, et al. "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE transactions on mobile computing, vol. 13, no. 6, pp.1268-1282, 2015. 15. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2014.
7. Y. Zhang, S. He, J. Chen. "Data Gathering Optimization by Dynamic Sensing and Routing in Rechargeable Sensor Networks," IEEE/ACM Transactions on network,doi:10.1109/TNET.2015.2425146, 2015.
8. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency,"IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.
9. S. Shen, H. Li, R. Han, et al. "Differential game-based strategies for preventing malware propagation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol.9, no. 11, pp. 1962-1973, 2014.
10. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2014.