Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 79 - 83. Submitted 01/11/2017. Published 13/12/2017

ACTIVE TRUST: SECURE AND TRUSTABLE ROUTING IN WIRELESS SENSOR NETWORK

[1]E. Akila, M.Phil Scholar, Bharathiyar Arts And Science College For Women, Deviyakurichi, Thalaivasal, Salem.

[2]C. Renuga, HOD, Bharathiyar Arts And Science College For Women, Deviyakurichi, Thalaivasal, Salem.

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.

1. 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.

2. 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.

3. RELATED WORK

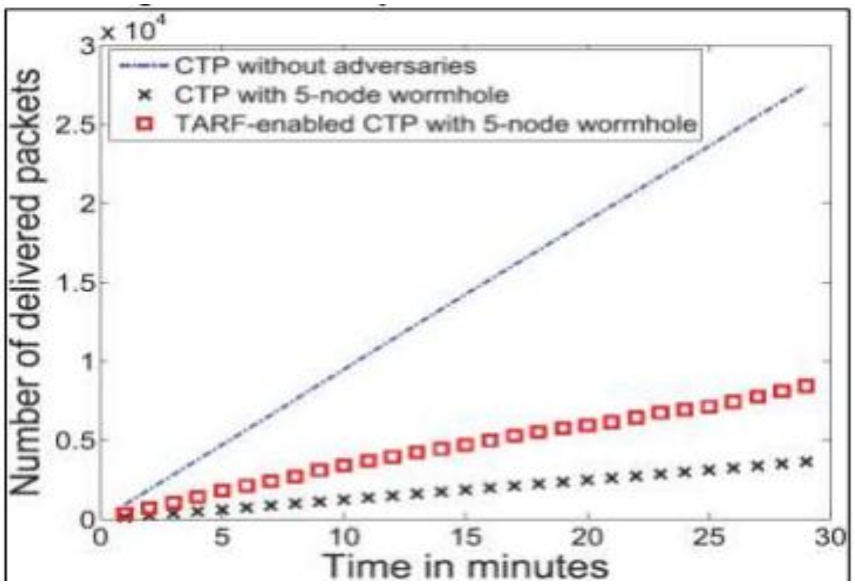

Fig.1.Collection Routing Protocol

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.

4. PROPOSED SYTEM

For a TARF [4] enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the reliability and the energy efficiency. Once the data packet has been forwarded to the next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decisions are made by its next-hop node.

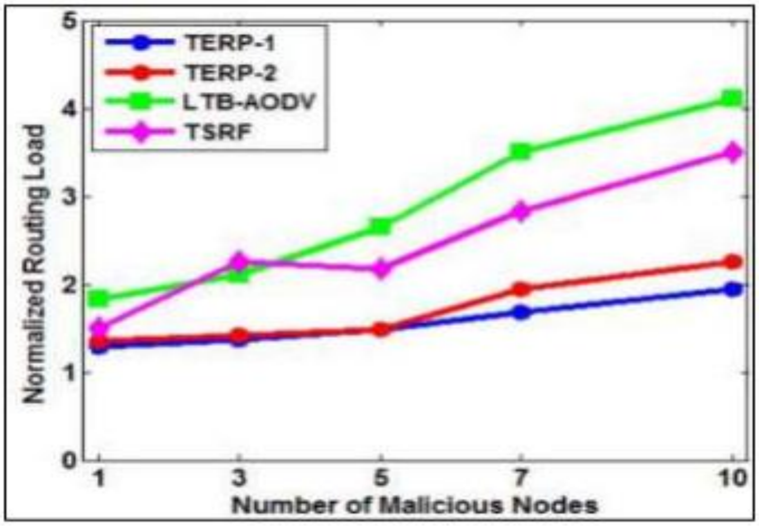

Fig.2.load Comparison

The node N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. EnergyWatcher is accountable for recording the energy cost for each known neighbor, based on N's surveillance of one hop transmission to reach its neighbors and the energy cost report from those neighbors. TrustManager is responsible for tracking the neighbors trust level values based on network loop discovery process and broadcast messages from the base station about data delivery. Once N is able to choose its next-hop neighbor according to its neighborhood table, it sends out its energy report message. Its energy cost is broadcasted to all its neighbors to deliver a packet from the node to the base station. During the route construction phase, the sink node broadcasts Route Construction (RCON) packets to its neighbouring nodes. The neighbouring nodes receive the RCON packet from the sink node. A neighbouring node updates RCON packet with its public key. It rebroadcast the RCON packet to its neighbouring nodes. Similarly all the nodes update their routing table with the public key of their neighbouring nodes in the network. In the data transmission phase, the source node will select node-disjoint paths to the sink node and sends the data traffic through that path.

5. ANALYSIS

The source node picks M amount of data to send through the node-disjoint primary path to the sink. The MD5 hash function H is used to create message digest H(M) from the M amount of data at the source node. The source node generates the digital signature by encrypting the message digest H(M) with its private key. The source node forwards it to neighbouring node through the path it takes to reach sink. A neighbouring node verifies the digital signature by comparing decrypted value.

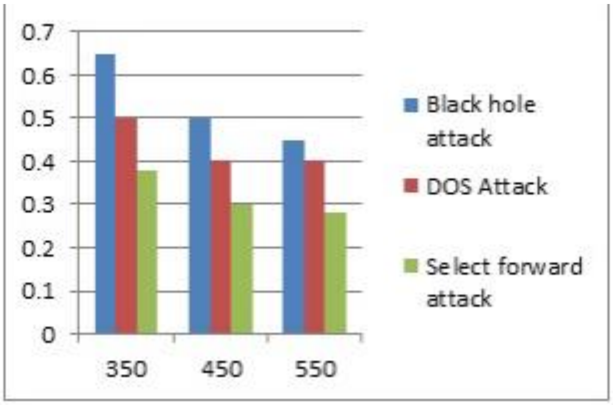

Fig.3.Output

If the generated H(M) by the receiver and the decrypted H(M) of digital signature is equal, then the receiver accepts the data. Otherwise rejects the data and informs the sender that the data is altered through by generating route error packet. In Fig. 3, as compared to the AOMDV model , the Packet Delivery Fraction (PDF) is always high in the EENDMRP model. The number of dropped packets in the EENDMRP model is less than that in the AOMDV model. In the EENDMRP model, the PDF is an average of 7% higher as compared to the AOMDV model because of queue buffer overflow. The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs. The difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink. Node a in the route will choose the neighbor.

CONCLUSION

In this paper, we have analyzed a various novel security and trust based routing scheme against black hole attack and presented their performance over the packet delivery ratio. From the above analysis, we can conclude that ActiveTrust scheme is the efficient scheme for detecting and preventing the black hole attack among other schemes. The ActiveTrust scheme has the following excellent properties: (1) High successful routing probability, security and scalability. The ActiveTrust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. (2) High energy efficiency. The ActiveTrust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that this scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, ActiveTrust scheme improves both the energy efficiency and the network security performance. It provides important significance for wireless sensor network security.

REFERENCES

[1] Yuxin Liu, Mianxiong Dong,Kaoru Ota, and Anfeng Liu, “ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks”, IEEE Transactions On Information Forensics And Security, Vol. 11, No. 9, PP. 2013 – 2027, September 2016.

[2] Tao Shu, Marwan Krunz, and Sisi Liu, “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes ,” IEEE Transactions on Mobile Computing, Vol.9,No.7,PP.941-954,July 2010.

[3] Ming-Yang Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems” ,Elsevier-Computer Communication,Vo;.34, pp-107-117, August 2010. [4] Guoxing Zhan, Weisong Shi and Julia Deng, “Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs”, IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, PP.184-197, April 2012.

[5] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection” , IEEE Transactions On Network And Service Management,Vol.9, No. 2, PP.169-183, June 2012.

[6] Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen and Xuemin (Sherman) Shen, “Secure and Energy-Efficient Disjoint Multipath Routing for WSNs,” IEEE Transactions On Vehicular Technology, Vol. 61, No. 7, PP. 3255-3265, September 2012.

[7] Shiva Murthy G, Robert John D’Souza, and Golla Varaprasad, “Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks”, IEEE Sensors Journal, Vol. 12, No. 10, PP.2941 -2949, October 2012.