International Journal of Computer Applications (0975 - 8887)
Volume 180 - No.41, May 2018

Efficient Trusted Model in WSN for Privacy Preserving

Komal Ligade
Department of Computer Engineering
SKNCOE, Vadgaon, Pune
Savitribai Phule, Pune University

S. P. Pingat
Professor
Department of Computer Engineering
SKNCOE, Vadgaon, Pune
Savitribai Phule, Pune University

ABSTRACT

In wireless sensor networks (WSNs), many factors, for instance, mutual interference of wireless connections, battlefield applications and nodes presented to the environment without top physical safety, effects in the sensor nodes being extra powerless in against to the attacked compromised. For tackling the issues security, an effective appropriated trust model is proposed. They faces some issues, first is system was not focus on other trust metrics Trust is evaluated by the two ways direct and indirect trust on the basis of recommendation from third party. The third issue is offering the trust assessment on neighbour nodes become very essential. Fourth, trust relationship between sensor nodes frequently modified in wireless sensor networks because of the dynamic topology. For solving all these issues proposed the efficient distributed trust model for wireless sensor networks. This system can estimate dependability of sensor nodes more accurately and prevent the security breaches more considerably. Also for sending the data from subject node to object there are number of paths are generated, in this system we used Dijkastra algorithm for finding the shortest path. Also for the existing system faces the problem of security against the different attacks on network. For security purpose we used ECC algorithm. Experimental result shows that energy consumption for proposed system and existing system.

Keywords

Trust management, Security in Wireless Sensor Networks, Direct Trust, Indirect Trust, Shortest Path Calculation.

1. INTRODUCTION

Network security is a non specific name for the accumulation of devices intended to ensure data and to thwart programmers. Network security establishes to ensure information during their transmission. Internet security establishes to ensure information their transmission over an collection of interconnected systems. Security attack is any activity that bargains the security of data possessed by an association. Security system is a procedure that is intended to recognize or recover from a security attack. Security services are a processing or correspondence benefit that improves the security of the information handling frameworks and the data transfers of an association. Threat is a potential for security, which exists when there is a situation, ability, activity, or event that could breach security and cause harm. That is, a risk is a conceivable threat that may exploit helplessness. Attack is an danger on framework security that gets from a intelligent framework; that is, an intelligent demonstration that is a deliberate attempt to evade security benefits and violate the security approach of a framework cryptography, verification, secrecy, and message integrity these security technique are used to avoid avoid security problems. For build secure connection, have a all communicating nodes are trusted. It is solved in our this system to demonstrate Efficient Distributed Trust Demonstrate (EDTM)[1].

In the proposed framework while calculating the trust focus on the some factors like: communication behavior, other trust metrices like energy level which should be calculated dependability of sensor nodes. For tackling the previously mentioned issues, we propose an effective distributed trust demonstrate (EDTM).The proposed system evaluate the trust connection between nodes. Also introduce Dijkstra algorithm for finding the shortest path to send the data from subject node to object node. Also we are focus on the security of data and network by using the ECC algorithm.

We discussed some concepts of trust:

(1) Direct Trust
This trust can be calculated based on direct communication. That shows the trust relationship between two neighbor nodes.

(2) Recommendation Trust
As stated above, the recommendations from third party not always reliable . So we want efficient mechanism to filter the recommendation information. Then the recommendation trust is calculated based on filtered reliable recommendations.

(3) Indirect Trust
When a subject node cannot directly observe an object nodes communication behaviors, indirect trust can be established.

2. REVIEW OF LITERATURE

In this section discuss the literature review in detail about the trust calculation on wireless sensor network.

In paper [1] , author proposed a Efficient Distributed Trust Model (EDTM) for WSNs. Firstly, sensor node obtain packets according to the numbers. That time direct trust and recommendation trust are observed. Then other trust are considered at the time of assessing direct trust. Also, trust reliability and shared commonality are described to upgrade the precision of recommendation trust.

H. S. Lim et. al. [2], proposed the proficient methods for estimating the reliability of data items. This method uses the data attribution and furthermore their qualities in processing trust scores, that is, quantitative measures of dependability. For obtain the trust score, author proposed a cyclic technique which was shows the interdependency reliance property: the trust score influence the trust score of the sensor node which controlled the information. The trust score of data items are calculated from their significance comparability and attribution similarity.

K. Govindan et. al. [3] signifies a detail summary on distinct trust computing techniques which are modified towards MANETs. Author outlines the overview and correlation of different methodologies. Moreover, author analyze distinct work done on trust flow including trust propagation, forecast and aggregation algorithm, the collusion of network dynamics on trust flow and the effect of trust on security.

G. Han et. al. [4] proposed a cross layer improved geographic node disjoint multipath routing algorithm, which is, two phase geographic greedy forwarding plus. To improve the framework, these algorithms are designed based on the multiple layer communications. There are three steps of the introduced system: first one is the physical layer in which sensor nodes are generated for searching the energy from environment, which is called as node rechargeable operation. Each node can exchange its transmission power on the basis of its present energy level. Second is the sleep scheduling layer, in which a energy controlled a sleep scheduling scheme, duty cycle and energy consumption on the basis of associated neighbourhood is associated for permitting sensor nodes to have the enough time for recharge the energy which takes nodes present energy level as the parameter to progressively schedule nodes to be dynamic on the other hand asleep. Third is the routing layer, in which a forwarding node selects the following next hop node based on 2-hop neighbor data as opposed to 1- jump.

K. Nordheimer et. al. [5] proposed a technique that interpreted trust as probability and can calculated neighborhood trust values on large network using a monte carlo simulation techniques. The assessment depending upon existing techniques of trust proclamation among the two users. This technique is at that point stretched out to the SimTrust evaluations that merge both the trust and doubt values.

Viljanen et al [6] deal with the all kinds of techniques used to calculate the trust after research of ten years on trust evaluation of network in which they are guiding for effect on trust evaluation of the sensor nodes in wireless sensor networks.

Viljanen et al [7] ,author proposed trust evaluation model and this model used simple statistical method methods.It cannot show nodes realtime trust state accurately. Ganeriwal et al.

Abdul-Rahman and Hailes in [8] proposed a model for supporting trust in virtual communities, based on direct experiences and reputation. They use direct and indirect (recommendations) trust and they introduced the semantic distance of the ratings in their mode.

Garth et al.[9] , author proposed a distributed trust-based framework. This model uses direct and indirect information coming from trusted nodes. weighting mechanism can be used for trust modelling. Trust table stored by each node and values are reported to the cluster head.

In paper [10] , author propose a trust model for identify the trusted sensor node. This paper shows each sensor node has knowledge , synchronised time and nodes are deployed.

In paper[11] ,author developed Sensor Rank mechanism. A network voting algorithm also proposed to determine faulty sensor readings.

3. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

3.1 Proposed System Overview

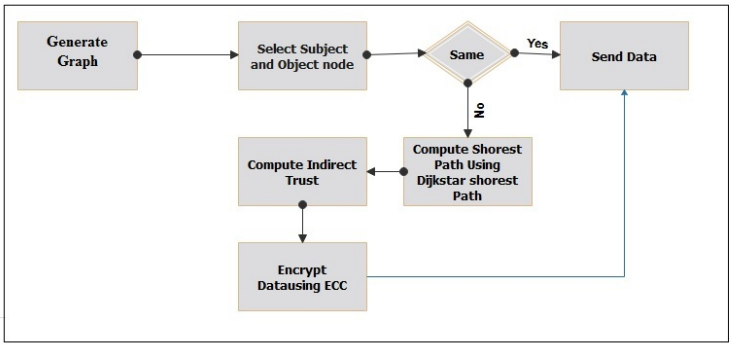

Fig. 1. System Architecture

Techniques used to implement this system:

—Network Generation
Initially, network is created with fixing the position of vertices/nodes. These nodes are connected with the edges. All nodes are initializing with equal amount of energy. Also subject node and object is selected.

—Path Generation
After creating the subject and object node, create every probable paths from subject node using Dijkstra?s algorithm. In this step each node creates its routing table. This table contains all path reached to object nodes.

—Get Shortest Path
Routing tables of all sensor nodes are collected at object node. This object node select the path with smallest distance receive data.

—Trust value calculation
There are two types of trust calculated of each node. In this system we are calculated indirect trust for each node in the shortest path.

—Key generation and distribution
Using key generation algorithm, key pair is generated for all sensor node and allocate to them. Every node will use this keys for encrypting data before forwarding it to next sensor node or object node.

—Data Encryption and data sending
The information sensed by sensor is encrypted before forwarding it, to sensor node. ECC algorithm is used for encryption and

decryption of information at subject and object end respectively. After encryption data is send to object node with the shortest path successfully.

3.2 Mathematical Model

3.3 Mathematical Model

System S is represented as
S= {N, S, R, Sp, T, D} Process:

(1) Deploy nodes
N = {N1, N2, ... ,Nn}
N is set of all deployed nodes.

(2) Select Subject Node and Object Node
S = {U, O}
Where, S is set of Subject Node and Object Node and U = {U1, U2,....,Un}
Where, U is a set of all Subject Nodes and O = {O1, O2,....,On}
Where, O is a set of all Object Nodes.

(3) R = range between subject node and object node.

(4) Select Shortest Path Sp = {Sp1, Sp2, Sp3, ...,Spn}
Where Sp is the set of all Shortest Path.

(5) Calculate Trust T = { T_{com}, T_{ene}, T_{Data} , $T_{n-direct}$, T_{rel} , T_{fam} , $T_{n-recom}$, $T_{n-indirect(^{B}_{Ci+1})}$}
Communication Trust T_{com}
The T_{com} is calculated on the basis of successful and unsuccessful packets. The formula for trust communication is as follows:

$$T_{com} = \frac{2b+u}{2}$$

Where b = $\frac{s}{s+f+1}$, u = $\frac{1}{s+f+1}$

Energy Trust T_{ene}
The T_{ene} is calculated as:

$$T_{ene} = \begin{cases} 1-P_{ene}, if E_{res} \geq \theta \\ 0, else, \end{cases}$$

Where P_{ene} is calculated based on the Ray Projection Model [9].
Data Trust T_{Data}
The trust value of the data is calculated as:

Where, f(x) = $\frac{1}{\sigma\sqrt{2\Pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$
x is the attribute value Vd of a data item,
μ, σ are mean and variance of the data.

Direct Trust $T_{n-direct}$
Direct trust value is calculated as:

$$T_{n-direct} = w_{com}T_{com} + w_{ene}T_{ene} + w_{data}T_{data}$$

Where,
w_{com}= Weighted value of the communication trust
T_{com}= Communication Trust
w_{ene}= Weighted value of energy trust
T_{ene}=Energy trust
w_{data}= Weighted value of energy data
T_{data}=Energy data

Recommendation Reality T_{rel}

$$T_{rel}=1-|T^{B}_{Ci} - T^{B}_{ave}|$$

Where, $T^{B}_{Ci}$is the recommendation value of object node B reported by recommender Ci.
T^{B}_{ave} is the average value of all recommendations.

Recommendation Familarity T_{fam}

$$T_{fam}= \frac{num^{B}_{Ci}}{num_{Ci}} \times \alpha^{\frac{1}{num^{B}_{Ci}}}$$

Where, num^{B}_{Ci} is the successful communication time between Ci and object B.
$num_{Ci}$is the total successful communication time of the recommendation
α is the regulatory factor of the communication times.

Recommendation Trust $T_{n-recom}$

$$T_{n-recom} = \frac{\Sigma^{n}_{i=1} 0.5 + (T^{B}_{Ci}) \times T_{rel} \times T_{fam}}{n}$$

Where, n is the number of recommender.

Indirect Trust $T_{n-indirect(^{B}_{Ci+1})}$

$$T_{n-indirect(^{B}_{Ci+1})} =$$

$$T_{Ci+1} \times T_{n-indirect(^{B}_{Ci})}$$

$$if(T_{n-indirect(^{B}_{Ci})}) < 0.5$$

$$0.5 + (T_{Ci=1} - 0.5) \times (T_{n-indirect(^{B}_{Ci})}), else$$

Where, n number of recommendation

$$TrustT_{n-indirect(^{B}_{Ci+1})} =$$

$$T_{Ci+1} \times T_{n-indirect(^{B}_{Ci})}$$

$$If(T_{n-indirect(^{B}_{Ci})}) < 0.5$$

$$0.5 + (T_{Ci=1} - 5) \times T_{n-indirect(^{B}_{Ci})}, else$$

$$where, (T_{n-indirect(^{B}_{Ci})}) = T_{C1} \times T^{B}_{c1},$$

$$if T^{B}_{c1} < 0.5 + 0.5 + (T_{C1} - 0.5) \times T^{B}_{c1} else$$

(6) Data Sending $D = \{D1, D2, D3, ...Dn\}$
Where, D is a set of all data transmitted.

3.4 Algorithm Used

Algorithm of the proposed strategy works as:

3.4.1 Algorithm 1: Proposed algorithm

(1) Generate a network graph as Graph G(V,E) where; V are vertices/nodes and E are edges.
(2) Select subject and object node.
(3) Generate all paths from subject to object node.
(4) Compare the node
(5) If node are same, send the data directly

(6) Else
(7) Compute shortest path from subject to object node by using Dijkstra Algorithm.
(8) Compute indirect trust for each node in the path. Technique for indirect trust calculation is discussed in mathematical section.
(9) Generate public/private keys and distributes to subject and object node.
(10) Encrypt the data with the private key.
(11) Send data to object node.

In the above algorithm explains the steps of the proposed system. Initially generate the graph with G(V,E) in which V is as a Vetices/nodes and E as a edges. After select that subject and object node from which data is send, compare the node if node is same send data directly. If the node are not same, compute the shortest path from subject to object node by using Dijkstra algorithm. Compute the indirect trust for each node in the path. Encrypt data using ECC algorithm and send data to object node.

3.4.2 Algorithm 2: Algorithm used for Encryption

(1) Sender and Receiver Calculated B = S = (S1, S2).
(2) Sender sends a message M E to Receiver as follows:
(3) Calculate (S1 $*$ S2) mod N = K.
(4) Calculate K $*$ M = C, and send C to Sender.
(5) Receiver receives C and decrypts it as follows:
(6) Calculate (S1 $*$ S2)modN = K.
(7) Calculate (K-1)modN.
(8) (Where N = E)
(9) K-1$*$C = K-1$*$K$*$M = M.

4. RESULTS AND DISCUSSION

4.1 Experimental Setup

—Software Requirements:
The system is built using Java framework jDK 1.8 on Windows platform. The Net beans IDE 8.2 is used as a development tool. Jung Simulation used for network creation. The system doesnt require any specific hardware to run; any standard machine is capable of running the application.

4.2 Experimental Result

In this section discussed the experimental result of the proposed system. Table I depicts the comparison of existing and proposed system on the basis of energy consumption. Proposed is more efficient than existing system. Fig. 2 demonstrates the comparison graph of energy consumption of proposed system and existing system. The energy spent of a node that transmits l-bits packet over distance d is:

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = E_{elec} * l + \varepsilon_{fs} d(2) * l$$

Where,

$$d_0 = \sqrt{\frac{\varepsilon_{f8}}{\varepsilon_{mp}}}$$

and the energy consumption of receiving this message is:

$$E_{Rx}(l) = E_{elex} *$$

Fig. 3 shows that the existing system takes maximum time to forward the data from source to destination node that the proposed

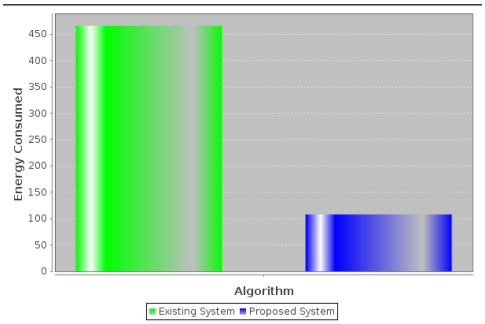

Fig. 2. Energy Consumption Graph

Table 1. ENERGY COMPARISON

System	Energy in Jules
Existing System	23000
Proposed System	10000

system. Table II shows the comparison of existing DBF and proposed system Dijkstar?s on the basis of time to forwarding data. Proposed is more efficient than existing system.

Table 2. TIME COMPARISON

System	Time in MS
Existing System	77
Propose System	58

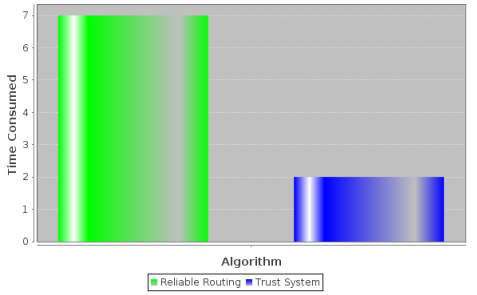

Fig. 3. Time Consumption Graph

The graph in Fig. 4 shows that the proposed system having minimum amount of packet drops than the existing system, because the proposed system uses trust score calculation of all nodes. Only node with the highest trust is considered for further data transmission. Therefore, the probability of packet loss at trusted node will be reduced. Table III depicts the comparison of existing and proposed system on the basis of average packet drop. Proposed is more efficient than existing system.

Table 3. Average packet drop comparison

System	Time in MS
Existing System	80
Propose System	60

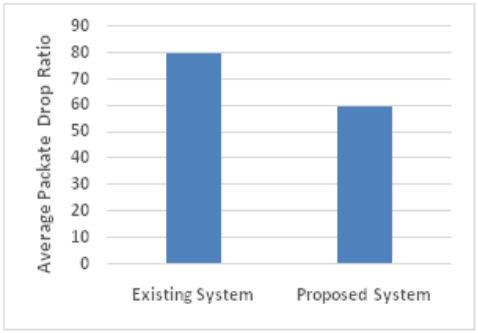

Fig. 4. Average packet drop ratio graph comparison

4.3 CONCLUSION AND FUTURE SCOPE

In wireless sensor network evaluating the trust model for the malicious node has become significant topic for researchers. To build up the trusted network can utilize in distinct applications such as secure routing, secure data aggregation, and trusted key exchange. In this paper, a distributed and efficient trust model named EDTM was proposed. During the EDTM, the calculation of direct trust, recommendation trust and indirect trust are discussed. Also for finding the shortest path for sending the data from subject node to object node system used Dijkstra algorithm, from which data can send fast and securely. For the security purpose system used ECC algorithm. In experimental result system were discussed about the comparison among the energy consumption for proposed system and existing system. In future we are tackling the issue of how to select the proper value of the weight and the defined threshold which is still a challenging problem.In this section, the author(s) should also briefly discuss the limitations of the research and Future Scope for improvement

5. REFERENCES

[1] Feng Wang, and Guangjie Han, “An efficient distributed trust model for wireless sensor networks”, IEEE Transactions, Vol. 26, NO. 5,[May 2015].

[2] H. S. Lim, and E. Bertino, “Provenance based trustworthiness assessment in sensor networks,” 7th Int. Workshop Data Manage. Sens. Netw., 2010, pp. 2-7[2010].

[3] P. Mohapatra and K. Govindan, “Trust Computations and Trust Dynamics in Mobile Dd Hoc Networks: A survey,” IEEE Commun, vol. 14, no. 2, pp. 279-298, [2012].

[4] G. Han, and D. Wu, “Cross-Layer Pptimized Routing in WSN With Duty-Cycle and Energy Harvesting?, Wireless Commun. Mobile Comput., DOI: 10.1002/ wcm, [2014].

[5] D. Veit, and T. Schulze, “Trustworthiness in Networks: A Simulation Approach for Approximating Local Trust and Distrust Values,” IEEE Commun., vol. 321, pp. 157- 171, [2010].

[6] L. K. Balzano and M. B. Srivastava, “Reputation Based Framework for High Integrity Sensor Networks”, in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., pp. 66-77, [2004].

[7] D. Kim, and Y. Doh, “PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security,” IEEE Int. Conf. Mobile Adhoc Sensor Syst., pp. 437-446,[2008].

[8] G. Ha and D. Wu, “Cross-layer optimized routing in WSN with duty-cycle and energy harvesting”, Wireless Commun. Mobile Comput., DOI: 10.1002/wcm.2468, [2014]

[9] S. Hailes and A. Abdul-Rahman and “Supporting Trust in Virtual Communities”, in The 33rd Hawaii International Conference on System Sciences, Maui, Hawaii, [2000].

[10] R. Ismail, and A. Jsang “The Beta Reputation System”, in The 15th Bled Electronic Commerce Conference. Bled, Slovenia,[2002].

[11] G. V. Crosby, and N. Pissinou “A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks”, in The Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, Columbia, Maryland, [2006].

[12] N. Pissinou and G. V. Crosby, ”Cluster-Based Reputation and Trust for Wireless Sensor Networks”, in The 4th IEEE Consumer Communications and Networking Conference (CCNC’07) Las Vegas, Nivada, [2007].