International Journal of Engineering & Technology, 7 (3) (2018) 1700-1704

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.15366
Research paper

Trust based secure de-forestation and timber theft alert in wireless sensor networks

P. N. Renjith

Associate Professor, School of Computing Sciences, Hindustan Institute of Technology and Science
**Corresponding author E-mail: pn.renjith.it@gmail.com*

Abstract

Deforestation is the permanent destruction of trees for timber and land. Deforestation and timber theft ends up with obliteration of entire forest in the earth. Deforestation has increased exponentially increase in this decade. It is well known that Deforestation is a prime reason for global warming, less tropical rainfalls and affects atmospheric oxygen level. In this paper, a novel query-based method has been introduced to alert deforestation to forest official. Trust analysis and data aggregation has been incorporated to improve security and fast transmission of information to the base station. Query based technique is used to evaluate the intrusion has been implemented. Simulation result proven that the ST-alert able to detect the trespasser and stop them from deforestation.

Keywords: *Deforestation; Wireless Sensor Networks; Trust Management; Data Aggregation.*

1. Introduction

India has well known for its natural beauty and dense forest. Human being depends extensively on forest for food, medicine, wood and shelter. Exponential increase in population results in increase demand wood, food, medicine and shelter. Result in deforestation. The total forests area of the world in 1900 was estimated to be 7,000 million hectares which was reduced to 2890 million hectares in 1975 fell down to just 2,300 million hectares by 2000. Deforestation is a continuous process in India where about 3.3 hectares of forest land has been lost. The per capital availability of forest in India is 0.08 hectares per person which is much lower than the world average of 0.8 hectares. The presence of waste land is a sign of deforestation in India. After 2001 it is found deforestation has been increased exponentially. Lot of trees has been cut down for construction purpose. Forest pirate become a key issue for deforestation. Even though we have strict measures to stop deforestation, pirates cut down the trees and sell them. Hence, we require an automated technique to stop deforestation. Wireless Sensor Network can be a better solution for deforestation. Wireless sensor networks comprised of huge number of low cost and limited-energy sensing devices. The chief operations of wireless sensor networks are sensing the environment, data sampling, computing and broadcasting the sensed information. But, sensor nodes have heavy resource limitations such as battery power, storage, processing capability, operating radio frequency, and bandwidth. It is hard to offer effective data gathering solutions. Numerous tiny and cheap devices are involved in the sensor networks that are capable of self-organizing ad hoc systems through which the information is collected and transmitted to one or more sink nodes by observing the physical environment. Thus, the data needs to be transmitted towards the sink node in a hop-by-hop manner. If the amount of data which needs to be transmitted is reduced, the energy consumption of the network is also minimized. To minimize this issue data aggregation technique is used in a wireless sensor network [1]. Data aggregation is a technique of clustering the data from multiple sensor nodes by eliminating the redundant data transmission which is then sent to the base station, thus it enhances the network performance and provides effective bandwidth utilization. Various data aggregation techniques are the centralized approach, tree Based approach, cluster based approach and in-Network approach [2].

2. Literature review

According to the features of WSNs, it is not possible to provide a centralized trust-based system as the centralized trusted center need to manage the entire systems in the network. When the size of network increases, a single centralized trusted center minimizes the scalability and flexibility of the WSNs. Thus, decentralized trust-based methods are applied in sensor network. The trust-based methods of WSNs are classified into five categories based on access, routing, location, and aggregation. The proposed method is developed using the concept of EDAT protocol which provides substantial benefits as it considers energy efficiency, communication link availability for trust computation.

Zeng, et al, [3] focused on providing suitable taxonomy of in-network aggregation. Several existing in-network aggregation techniques, their drawbacks and the solutions were discussed. Boukerche and Ren [4] proposed a trust computation and management system (TOMS) to create a generic trust model for assessing the nodes activities such as credential assignments, managing the trust values, key updating, and decision making. Ganeriwal et al, [5] presented reputation-based framework for high integrity sensor network (RFSN) which is a first trust based model designed and developed for sensor networks. It makes use of watchdog mechanism to collect data and monitor different events in the node to build reputation of the node and then get the trust rating of the node. The TMF [6] is a dynamic trust management framework which reduces communication overhead, computation overhead and memory requirements by combining both behavior and certificate based scheme. Shaikh et al. [7] proposed hybrid trust management architecture for clustered WSNs, which they called GTMS. The reputation values are evaluated at sensor node level, cluster head level and base station level which is the key benefit of GTMS method. The TMA [8] is dynamic certification based trust management architecture for hierarchical WSN that minimizes the computation and communication overhead by considering behavioral as well as the direct trust. The reliable data aggregation and transmission protocol (RDAT) is a distributed functional based beta reputation model that computes the reputation and trust values for depending on three precise aspects such as aggregating, sensing and routing [9]. It increased the reliability of data aggregation and transmission by assessing sensor node action through functional reputation and eliminated false injection /compromised attack.

Sirsikar, S., & Anavatti, S [10] focused on various issues with respect to data aggregation processes such as delay, redundant data elimination and reliability. And various existing data aggregation has some different issues like redundancy, delay, accuracy, and traffic load. And these issues affect the performance of data aggregation. A two stage data aggregation is performed with one at cluster head and the other at storage node to balance the energy efficiency and accuracy. Anna Felkner [11] presented a role based trust management language for distributed access control environment to represent security policies and credentials. Role Based Access control methods (RBAC) are based on RT language and RTD mention policies over sensor node which deputies their roles to some other node when they vary their location. It mentions the delegation on the basis of attributes. Umarani, V., & Sundaram, K. S [12] discussed trust models structure such as centralized, distributed and hybrid model. They also discussed the design issues attacks and the security mechanism. Then they performed a comparative analysis on several existing trust model. The agent-based trust model for Wireless Sensor Networks (ATSN) and Agent based Trust management (ATRM) [13] are agent based reputation approaches. In ATRM, distributed certificate based trust model monitor the behavior of network with the help of agent module. Agent module performs the reputation calculation by issuing t-certificate. Sensor node decides the transaction of node or not from mobile agent by issuing r-certificate. It addresses the uncertainty issue, but still cooperates with the malicious nodes and has one value of trust rating for different events.

3. Proposed system

Wireless Sensor Network will be established in the dense forest for finding unauthorised access in to the forest. The sensor nodes will be keep track of the entry of the unauthorised person. Once the person enters the particular area the information is sensed and send through multi hop routing to the base station. Base station in-turn alert the forest department to take necessary action. To improve the trust worthiness of the sensed information, Reputation and trust systems are developed to resolve the issues of cryptographic-based secure data-aggregation. They are used for detecting, gathering, processing, and disseminating the feedbacks regarding the sensors' activities and evaluating their trustworthiness for particular applications. These systems provide security against node capture attack and eliminating the compromised nodes involvement in data-aggregation. The trustworthiness of sensor nodes is computed depending on their activities such as data collection, transmission, aggregator election, and path selection. Node reputation refers to the anticipation of neighbouring nodes regarding a node's behaviour based on previous observations. Thus, trust and reputation in a WSN are stated together. A node's anticipation will affect its adoptions and activities. Trust of a node is referred as the expected value of node's reputation.

In the proposed system, the cluster based WSN is used in which sensor nodes that are deployed are grouped into clusters. Figure 1 depicts the cluster-based data aggregation technique. Hence, the reputation and trust of the sensor nodes are evaluated only by the nodes in their own cluster. Efficient Distributed trust model is used to calculate the trust based on the number of packets received from sensor nodes in wireless sensor network. While calculating trust, communication trust, energy trust and data trust are considered. EDTM model detects the malicious nodes based on the trust value calculated.

3.1. Phases in proposed system

1) EDTM is applied for each node to calculate trustworthiness using direct trust. The nodes with high trust value are selected as a cluster head for the particular cluster. During trust calculation, three trust values are considered namely communication trust, data trust and energy trust.
2) Data of trusted nodes of cluster are sent to aggregator
3) Data from each aggregator are collected.
4) Data is forwarded to base station.

Each cluster has a cluster head called data aggregator which controls and coordinates some number of nodes. It is also responsible for aggregating the data from its member nodes.

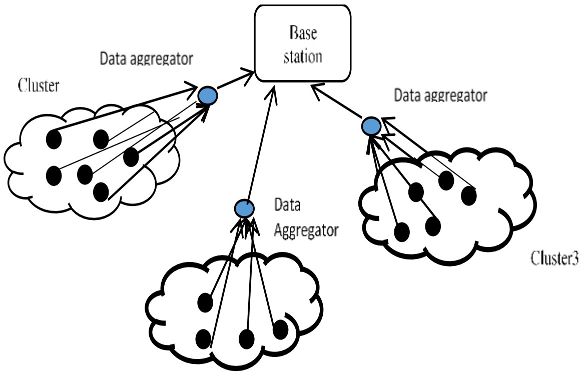

Fig. 1: Cluster Based Data Aggregation.

Aggregators are utilized to process received data from member nodes and transmit the aggregated results to the base station. The sensor nodes perform the sensing operation, observes other nodes, activities, exchange observations with neighbouring nodes, evaluate the trustworthiness of the nodes, and transmit data and observations to the aggregator. The data aggregators are varied dynamically based on trust value since the adversaries can trace the data aggregators. Also, the power consumption of the aggregators rises rapidly and significantly when they serve as aggregators for longer periods. Hence, to solve the security and power issues, sensor nodes in the cluster are re-elected aggregators dynamically.

3.1.1. Trust

Trust is defined as a belief level that one sensor node puts on another node for a specific action according to the previous observation of behaviours.

3.1.2. Trust in terms of energy (ET)

First, an energy threshold Eth is defined. If the residual energy E-residual of a sensor node is below the threshold value, then it does not possess enough energy. So the energy trust is set as 0. The energy trust is computed based on consumption of energy previously which is defined by Er,

$$ET = 1 - Ecr \text{ if } Eresidual \geq Eth \quad (1)$$

0 otherwise

When the energy consumption rate is large then the residual energy will be lowered, which results in reduced node capability for completing the task. If the energy consumption rate in previous time frames for an node is given by Ecr =(Ecr (1), Ecr (2)…. Ecr (n)) for n time frame.

The energy consumption at current time frame (n+1) is denoted Ecr (n+1),
Then the change in energy consumption rate is denoted by

$$\text{ECch-rate} = \text{Ecr}(i) - \text{Ecr}(i-1) \tag{2}$$

The node calculates ECch-rate for every consecutive time difference and computes the minimum of the value of ECch-rate. This minimum value is called the predicted energy consumption rate.
Trust (in terms of data)
The data packets have a spatial correlation, i.e., the packets sent among neighbor nodes are always alike in the same region. The data value of these packets follows a normal distribution. For a set of data, the probability density function is f(x)

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu')^2}{2\sigma^2}} \tag{3}$$

Here x is the attribute value vd of a data item, and μ and σ are mean and variance of the data, respectively.
As the mean is the most representative value that reflects the value similarity of the data, it has the greatest trust value. If the value of a data item is proximity to the mean, the trust value is moderately high, and the converse is true. Therefore, the trust value of the data item is defined as

$$D_T = 2(0.5 - \int_{\mu}^{a} f(x)dx) = 2\int_{a}^{\infty} f(x)dx \tag{4}$$

Trust (in terms of communication) (CT)
To deal with this uncertainty, the subjective logic framework is employed for resolving the issues of uncertainty [13]. The trust value in SL framework is represented as a triplet T = {B, D, U}, where B represent belief, D represent disbelief and U represent uncertainty.

B, D, U [0; 1] and B + D + U = 1.

Following the trust model based on Subjective Logic framework, the communication trust Tcom is calculated based on successful (s) and unsuccessful (f) communication packets:

$$C_T = \frac{2B + U}{2} \tag{5}$$

Where

$$B = \frac{S}{S + F + 1} \quad U = \frac{1}{S + F + 1} \tag{6}$$

3.1.3. Trust value updating

The nodes may enter or exit the network as WSN is highly dynamic behavior, the trust values of sensor nodes should be updated periodically. The repeated updating of the trust value results in wastage of energy. A node's historical trust values must be considered for computing its current trustworthiness. A sliding time window method is utilized for updating the trust value. The time window consists of many time slots for trust updating. Every slot indicates a cycle time in which, the node assesses the trust value of the node as T (i); i = 1,..m, where m is the number of time slots. In the next cycle time, the trust value is updated.

3.1.4. Cluster formation

AOnce the deployment is completed, the nodes broadcast their id and total trust value to their neighbors. When the participating the nodes discovered the neighbors, they exchange information regarding the trust value. The node which has maximum trust value is selected as the data aggregator for that cluster. Other nodes become members of the cluster. The nodes update the trust values accordingly

```
Cluster head selection
If (TT < TT prev)
For i= 1to n
Compute the energy trust (ET) which is given by equation 1.
Compute the data trust DT which is given by equation 2.
Compute the communication trust CT which is given by equation 3.
Calculate total trust TT = $\sum$ (ET + DT + CT)
Update the trust values ET, DT and CT of all nodes in cluster
End
For I =1 to n
Find the node with maximum trust value TT (max) as cluster head.
Broadcast to other nodes.
```

3.1.5. Deforestation and timber theft alert system

The WSN is established in the forest. The sensor nodes are enabled to tract the entry of unauthorised intruders. Once the sensor node encounters any unauthorised access, the information is sensed and spread around the network. The sensed information from multiple sensor are aggregated by the aggregator node and check for trust worthiness.

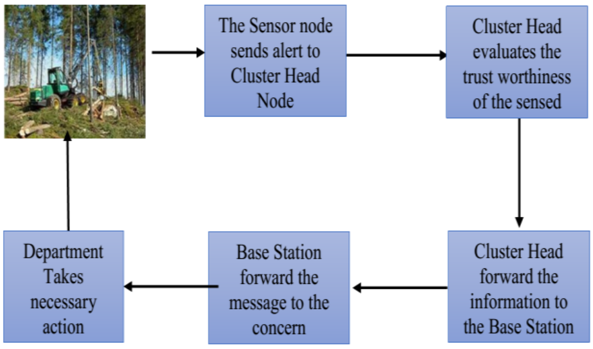
The Sensor node sends alert to Cluster Head Node
Cluster Head evaluates the trust worthiness of the sensed
Cluster Head forward the information to the Base Station
Base Station forward the message to the concern
Department Takes necessary action

Fig. 2: Working of Deforestation and Timber Theft Alert System.

Once the sensed information is found trusty, the information is passed to base station by multi-hop transmission. The information is send in the form of alert. Once the information is reach the base station, the same alert will be forwarded to forest department with priority (Severe, moderate or less threat). The necessary action can be done by the department. Query based technique can be utilized to evaluate total number of unauthorised access. A query is send to the base station, total number of people or vehicle crossed the specific region. The query will be send to the concern cluster head. Based on the aggregated information and time stamp total number of vehicle can be evaluate. Each sensed information is passed across a cluster head and the cluster head aggregates the information with the priority request. The trust value of the sensor node is evaluated before aggregating and then forwarded to the base station. The base station will get the cluster head location and the message. The user can send the queries to the cluster head for precise information. The table 1 represents the alert message format.

Table 1: Alert Message

Time	Message	Alert Priority
22.34	Unauthorised access	High

Query: Count * from Unauthorised_access where table_name= unauthorised_table
The query fetches total number of unauthorised access and the necessary action can be taken based on the count. The sensor nodes are provided with limited memory. Memory is flashed in hourly based. The backup of sensed information will be stored in the base station.

4. Performance analysis

Live test bed and The Network Simulator-2 (ns2) is used to simulate the network and access the performances of the proposed EDTM based clustering method. The accuracy of data aggregation is considered as an important factor in analysing the aggregation performance of the network. It is defined as the ratio of the sum of data from legitimate nodes gathered by the base station to the sum of data gathered by the base station. The data from sensors nodes of each cluster are securely aggregated to the base station through aggregator. By using EDTM the malicious nodes are detected and avoided based on the trustworthiness of the sensor node. The method is reliable, trust-based, energy-efficient, and secure. The Network lifetime of nodes for the proposed method and the trust based LEACH protocol are compared in figure 4. The proposed method provides a better life time than the TLEACH protocol.

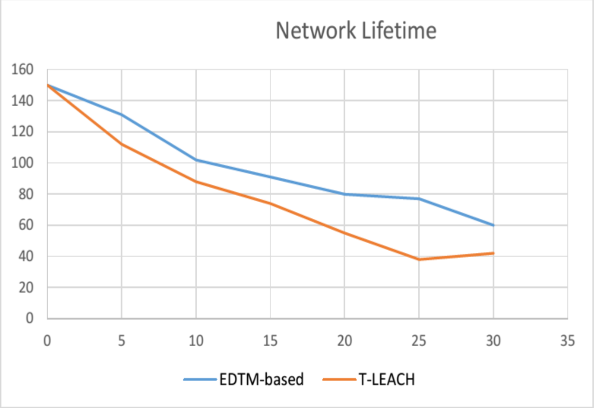

Fig. 4: Network Lifetime vs. Time.

The packet delivery ratio (PDR) of the proposed method and the trust based LEACH protocol are compared in figure 5 and it is proved that the proposed method provides a better PDR than the TLEACH protocol.

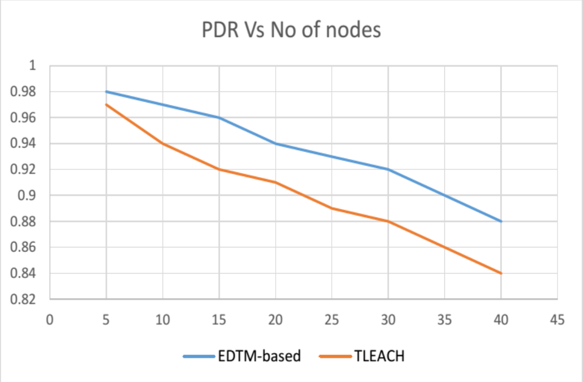

Fig. 5: PDR vs. Number of Nodes.

The reliability of the proposed method and the trust based LEACH protocol are compared in figure 6 and it is shown that the proposed method provides a better reliability than the TLEACH protocol.

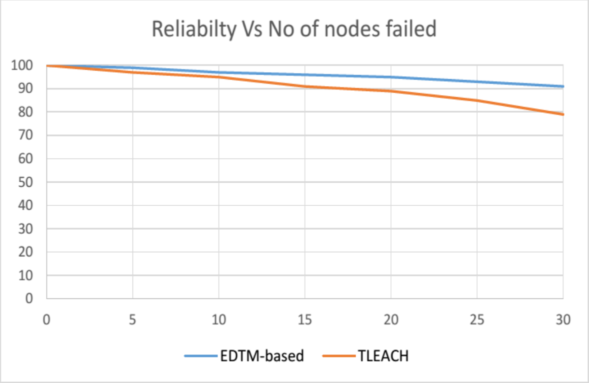

Fig. 6: Reliability % vs. Number of Nodes Failed.

4.1. Experiment on intrusion detection in live test bed

In the live test bed constructed with the MoteLab [14] and applied the algorithm and tested the intruder entering the specific region. The Site manager is made as the gateway sensor to forward the sensed information to the user interface. The site manager node act as the query forwarder and controller of the network. The algorithm is installed with wireless 802.11 Ad Hoc network control channel. The experimental result proven that intruders are easily tracked and forwarded to the user. Based on the severity of cumulative send data and accuracy, the user can send the information to the respective department to take a necessary action to control deforestation.

5. Conclusion

Deforestation become prime issue for the event of any country. It leads to unpredictable global climate change and end in extreme climate. to stop deforestation, the planned Deforestation and Timber thieving alert system plays a significant role. the need of trust in a very WSN is largely applicable for sensing, information revelation choices and key exchange. a brand-new approach to secure information aggregation technique by mistreatment the Efficient Distributed Trust Model (EDTM) is applied to cluster-based aggregation mechanism to avoid data falsification and to reduce the energy consumption. The simulation results proven that proposed methodology has be outperformed.

References

[1] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, *11*(6), 6-28. https://doi.org/10.1109/MWC.2004.1368893.

[2] Maraiya, K., Kant, K., & Gupta, N. (2011). Wireless sensor network: a review on data aggregation. *International Journal of Scientific & Engineering Research*, *2*(4), 1-6.

[3] Xu, J. X. J., Zeng, S. Z. S., & Qu, F. Q. F. (2006, November). A new In-network data aggregation technology of wireless sensor networks. In*Semantics, Knowledge and Grid, 2006. SKG'06. Second International Conference on* (pp. 104-104). IEEE.

[4] Boukerche, A., & Ren, Y. (2008). A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications*, *31*(18), 4343-4351. https://doi.org/10.1016/j.comcom.2008.05.007.

[5] Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *4*(3), 15. https://doi.org/10.1145/1362542.1362546.

[6] Zhang, J., Shankaran, R., Orgun, M. A., Varadharajan, V., & Sattar, A. (2010, December). A dynamic trust establishment and management framework for wireless sensor networks. In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on* (pp. 484-491). IEEE. https://doi.org/10.1109/EUC.2010.80.

[7] Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2009). Group-based trust management scheme for clustered

wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *20* (11), 1698-1712. https://doi.org/10.1109/TPDS.2008.258.

[8] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun Vijay Varadharajan and Abdul Sattar , 2010 A Trust Management Architecture for Hierarchical Wireless Sensor Networks , 35th annual IEEE conference on local computer networks.LCN ,pp. 268-273

[9] Suat Ozdemir, 2008 Functional reputation based reliable data aggregation and transmission for wireless sensor networks in Computer Communications, pp 3941–3953.

[10] Sirsikar, S., & Anavatti, S. (2015). Issues of Data Aggregation Methods in Wireless Sensor Network: A Survey. *Procedia Computer Science*, *49*, 194-201. https://doi.org/10.1016/j.procs.2015.04.244.

[11] Anna Felkner, 2011 How the Role-Based Trust Management Can Be Applied to Wireless Sensor Networks in journal of telecommunications and information technology, pp. 70 -78.

[12] Umarani, V., & Sundaram, K. S. (2013). Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks.

[13] Boukerche, A., & Li, X. (2005). An agent-based trust and reputation management scheme for wireless sensor networks. In *GLOBECOM'05. IEEE Global Telecommunications Conference, 2005*. (Vol. 3, pp. 5-pp). IEEE. https://doi.org/10.1109/GLOCOM.2005.1577970.

[14] G. Werner-Allen, P. Swieskowski, and M. Welsh. Motelab: a wireless sensor network testbed. In IPSN ’05: Proceedings of the 4th international symposium on Information processing in sensor networks, page 68, Piscataway, NJ, USA, 2005. IEEE Press. https://doi.org/10.1109/IPSN.2005.1440979.