RESEARCH ARTICLE OPEN ACCESS

Enhancing Security in Wireless Sensor Network Using Load Balanced Data Aggregation Tree Approach

A.Senthilkumar[1], K. Madhurabhasini[2]

[1](Asst.professor, Dept.of.Computer science, Tamil University (Established by the Govt.of.Tamilnadu), Thanjavur.)

[2](Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur.)

--************************----------------------------------

Abstract:

Trust is an important factor in transferring data from the source to destination in wireless AdHoc network. If any node un trust in the transfer the data, the Dynamic Source Protocol calculates the alternate path. Currently, the Dynamic Source Protocol does not have any built-in functionality to calculate an alternate path if the path has a malicious node. Intruder detection system can detect untrust worthy node. However, intruder detection system is very expensive for AdHoc networks and there is no guarantee in detecting a untrust node. In the current research, a trust-based approach is recommended to minimize the overheads of intruder detection system and detect the abnormal behaviour nodes. The data can be send and receive through set the path using the level based scheme to efficiently send the data to the receiver and the data rate can be increased and set the different path to send the data.

Keywords — **Adhoc,propagation.**

--************************----------------------------------

I. INTRODUCTION

Wireless Networks with scheduled intermittent connectivity, vehicular that disseminate location-dependent information and pocket-switched networks that allow node to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent dis-connectivity. In node transmission, the messages are also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the node trust strategy, and the routing is decided in an "opportunistic" fashion. In adhoc network a node could misbehave intentionally even when it has the capability to forward the data. Routing misbehaviour can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or untrust nodes that drop packets or modifying the packets to launch attacks. The recent researches show that routing misbehaviour will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance. Mitigating routing misbehaviour has been well studied in traditional ad hoc networks. These works use neighbourhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes.

Even though the existing misbehaviour detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficulty to predict mobility patterns, and long feedback delay have made the neighbourhood monitoring based misbehaviour detection scheme unsuitable for node. Since there may be no neighbouring nodes at the moment of the misbehaviour cannot be detected due to lack of witness, which renders the monitoring-based misbehaviour detection less.In network, clustering is used as an effective technique to achieve scalability, self-organization,power saving, channel access, routing etc. Lifetime of sensor nodes determines the lifetime of the network and is crucial for the sensing capability. Clustering is the key technique used to extend the lifetime of a network. Clustering can be used for load balancing to extend the lifetime of a sensor network by reducing energy consumption. Load balancing using clustering can also increase net work scalability. Network with the nodes with different energy levels can prolong the network lifetime of the network and also its reliability.

In this existing system the individual user data can be exchanged over the thirds party nodes. Individual data can be accessed through the third party server, and it can be out sourced. Before outsourcing, the secrecy data to be encrypt and outsource the data. In this system, the particular secrecy data can be maintained by the central authority (CA) to the trust management on behalf of node trust. In this system, the untrust behaviors which may lead to the exposure of the secrecy data. In Existing the access policy based mechanism is not used. The nodes are trusted blindly.

DISADVANTAGES:

- ❖ In this system, for the individual user having the central authority for the data transmission. Data unsafe.
- ❖ The Data can be accessed by the third party nodes and can be accessed by unauthorized users.
- ❖ Easily Compromised nodes and Reveals Secure Data.
- ❖ The sensitive applications demand secure transmission at the time of deployment of nodes.

PROPOSED SYSTEM:

In the proposed system, the secure sharing of secrecy data is storing on the trusted nodes in presence of Level based scheme by users. It can be protected using the trusted nodes and level based scheme can be used to trust the particular user data node as per the user needs. These works use neighbourhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to motivate rational nodes or revocation schemes to revoke malicious nodes. In this to improve security the user is categorized trusted node can be categorized. The data and increased the data rate and the net rate efficient schedule the data and the share the data efficiently.

ADVANTAGES:

- ❖ Good chance of bringing the source in contact with destination to nodes.
- ❖ High probability of message delivery to succeed.
- ❖ The source and destination come in contact with each other directly.
- ❖ Possible when the source and destination are one hop apart or immediate neighbor of each other.
- ❖ No global or local knowledge about network.

Pseudo code:

```
Step 1: Initialize the No of Levels and no of Nodes to construct a WSN network in Data Aggregation Tree
Step 2: Generate the no of levels with no of child in the tree
Step 3: Assign Level Key to each Level of the tree
Step 4: Assign each node key to each level in the tree.
Step 5: Each node can communicate from one level to another using Iterative Filtering.
Step 6: The Source node send info to Destination node by level key and node info key
Step 7: the Key gets updated in Hash Table.
Step 8: The recursive IF is used for secure communication
```

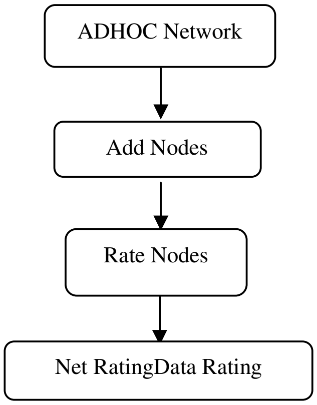
NETWORK FORMATION

Challenging your Neighbor is defined to trust and authenticate a new node, you can challenge your neighbor to add that node into the network. A node having its neighbors in its friend list does not need to challenge them before a data session.

Rate nodes: Initially each node has only those nodes in their friend list that completed the challenge successfully. Sharing of nodes is done in the Share nodes stage as the relation is transitive in nature that relative node of includes in his node list.

Data rating: The data rating is updated by a node for its friend on the basis of amount of data it transfers for it.

Net rating: FR represents the opinion of the friends of a particular node towards the integrity of another node, towards the integrity of another node, while DR represents a personal opinion of a node derived on the basis of previous data sessions. Both these ratings are important as certain nodes could be selectively malicious based on the holistic metric called as the Net Rating.



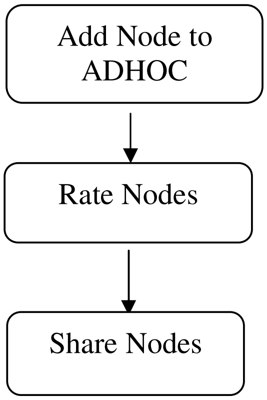
Share the Trust Nodes

Nodes sharing is a periodic process which is chiefly responsible for the security of the algorithm. To accomplish friend sharing we use the control packet FREQ (Friend sharing request). The node receiving the FREQ replies with the nodes in its friend list, unauthenticated list and the question mark list.

The rules for friend sharing are as follows.

- ➢ Any node can ask for a friend sharing request.
- ➢ After friend sharing, challenges are initiated for those nodes which were not in the friend list.
- ➢ If a node is already in the friend list the node updates its friend list.

After the friend sharing process is complete a node may start a data session or may sit idle.



Ensuring Security in Data Sharing Using level based scheme:

ECC is the most secured and advanced cryptography algorithm used for security in data sharing. The ECC algorithm can uses a key as small as possible is the main advantage. It helps to protect data sharing in each node of routing. The most common problem occurs in ECC is discrete logarithmic problem, which is used to increase complexity for attackers, Therefore the DLP is combined with ECC cryptography algorithm to ensure security in name of level based scheme.

Routing Efficiently

The data can be send through the single routing path the data sending and receiving time should be increased and the data rate can be decreased and data sharing performance can be delayed by the present using algorithms. The data can be send and receive through set the path using the SEGPSR algorithm to efficiently send the data to the receiver and the data rate can be increased and set the different path to send the data and increased the data rate and the net rate efficient schedule the data and the share the data efficiently**.**

5. CONCLUSION

` In this paper the result from simulation and comparison of various routing protocols such as First Contact and Direct Delivery. The data transmission between one nodes to another node using secure data transmission. The result shows that when we need to achieve higher delivery ratio it will increase the overhead ratio when numbers of nodes are increased. It requires more buffer space to replicate messages copies. When we replicate more copies it will achieve better delivery ratio but also requires much buffer space to store messages.

6. FUTURE ENHANCEMENT

The control technique for multilevel power converters can be further simplified and generalized to different levels and other class of power converters and inverters. The levels of multilevel configuration can be increased and further improvements in terms of performance and power quality. Data transmission, to avoid such thread, the nodes in the network are monitored by Trusted Authority and set a probabilistic value, the probabilistic value denotes the node trust. So the Probabilistic misbehavior Scheme is used for secure data transmission.

REFERENCES

[1]B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? Sentiment classification using machine learning techniques," in Proc.EMNLP, Philadelphia, PA, USA, 2002, pp. 79–86.

[2]B. Snyder and R. Barzilay, "Multiple aspect ranking using the good grief algorithm," in Proc. HLT-NAACL, New York, NY, USA, 2007, pp. 300–307.

[3]L. Tao, Z. Yi, and V. Sindhwani, "A non-negative matrix tri-factorization approach to sentiment classification with lexical prior knowledge," in Proc. ACL/AFNLP, Singapore, 2009, pp. 244–252.

[4]T. Wilson, J. Wiebe, and P. Hoffmann, "Recognizing contextual polarity in phrase-level sentiment analysis," in Proc. HLT/EMNLP, Vancouver, BC, Canada, 2005, pp. 347–354.

[5]J. Yu, Z.-J. Zha, M. Wang, and T. S. Chua, "Aspect ranking: Identifying important product aspects from online consumer reviews," in Proc. ACL, Portland, OR, USA, 2011, pp. 1496–1505.

[6] Bo Pang1 and Lillian Lee2Foundations and Trends in Information Retrieval Vol. 2, Nos. 1–2 (2008) 1–13

[7] S. Zhou, S. Zhang, and G. Karypis (Eds.): ADMA 2012, LNAI 7713, pp. 577–588, 2012.c_Springer-Verlag Berlin Heidelberg (2012)

[8] Baccianella, Stefano, Andrea Esuli, and Fabrizio Sebastiani. (2010).SentiWordNet 3.0: An enhanced Lexical resource for sentiment analysis and opinion mining. In Proceedings of the Seventh Conference on International Language Resources and Evaluation (LREC'10), pages 2200–2204, Valletta.

[9] Kessler, B., Nunberg, G., and Schutze, H. 1997. Automatic Detection of Text Genre. In Proc. of 35th ACL/8th EACL.