IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 57-58
www.iosrjournals.org

Client Based System on Wireless Sensor Network for Efficient Packet Transmission

Mr.S.Selvakumar[1], S.R, Manikandan2
[1]*(Assistant Professor, SRM university, India)*
[2]*(M.Tech CSE, College/ SRM university, India)*

Abstract : *Wireless sensor networks are vulnerable to the node distributor dividend, and several distributed protocols has been transfer the data in secure .Where MD5 algorithm that implements adaptive TTL, piggybacking, and perfecting, and provides near strong consistency guarantees. Cached data items are assigned adaptive TTL values that correspond to their update rates at the data source. Expired items as well as non expired ones but meet certain criteria are grouped in validation requests to the data source, which in turn sends the cache devices the actual items that have changed, or invalidates them, based on their request rates. In DHT-based protocol can detect node distributor dividend with high security level to transfer the data. Protocol of this type initial nodes send claiming messages containing a neighbor-list along with a maximum hop limit to randomly selected neighbors then, the subsequent message transmission is regulated by a probabilistic directed technique to approximately maintain a line property through the network as well as to incur sufficient randomness for better performance on communication.*

Keywords: *Message digestion, Time to live, Distributed hash table, Piggybacking, Prefetching*

I. Introduction

Wireless sensor networks (WSNs) have gained a great deal of attention in the past decade due to their application areas and formidable design challenges. It consists of hundreds and thousands of low-cost, resource-constrained, distributed sensor nodes, which usually scatter in the surveillance area randomly, working without attendance. If the operation environment is hostile, security mechanisms against adversaries should be taken into consideration for detect clone nodes. Among many physical attacks to sensor networks, the node clone is a serious and dangerous one. Because of production expense limitation, sensor nodes are generally short of tamper-resistance hardware components; thus, an adversary can capture a few nodes, extract code and all secret credentials, and use those materials to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that seem legitimate can freely join the sensor network and then significantly enlarge the adversary's capacities to manipulate the network maliciously.

II. System Proposed Work

The system is designed for the identification cached data items are assigned adaptive TTL values that correspond to their update rates at the data source. Expired items as well as non expired ones but meet certain criteria are grouped in validation requests to the data source, which in turn sends the cache devices the actual items that have changed, or invalidates them, based on their request rates.

1. Managing the request table

It describes the basic operation of Server side updating for the cache consistency in server-based approaches and how the request has been handled in the network.

2. *Network Traffic Analysis*

It deals with the nodes in the network. It shows how the network adapts itself to handle the disconnected. It also deals with the responsibility for maintaining and replacing of the cached data in the DHT table.

3. *Traffic Maintenance*

Traffic Maintenance keeps track of the Update rate and the Request rate of a particular data in the application data and server. Based on that the caching of data is done which reduce the traffic in the network.

4. Calculating the Nodes Life Times

It will calculate the life time of each and every node in the network. The user may get the information about which node is under network transmission and still living and which one is expired those information will be processed in TTL logic and grouping the expired nodes into one and transmit it once again.

III. Figures And Tables

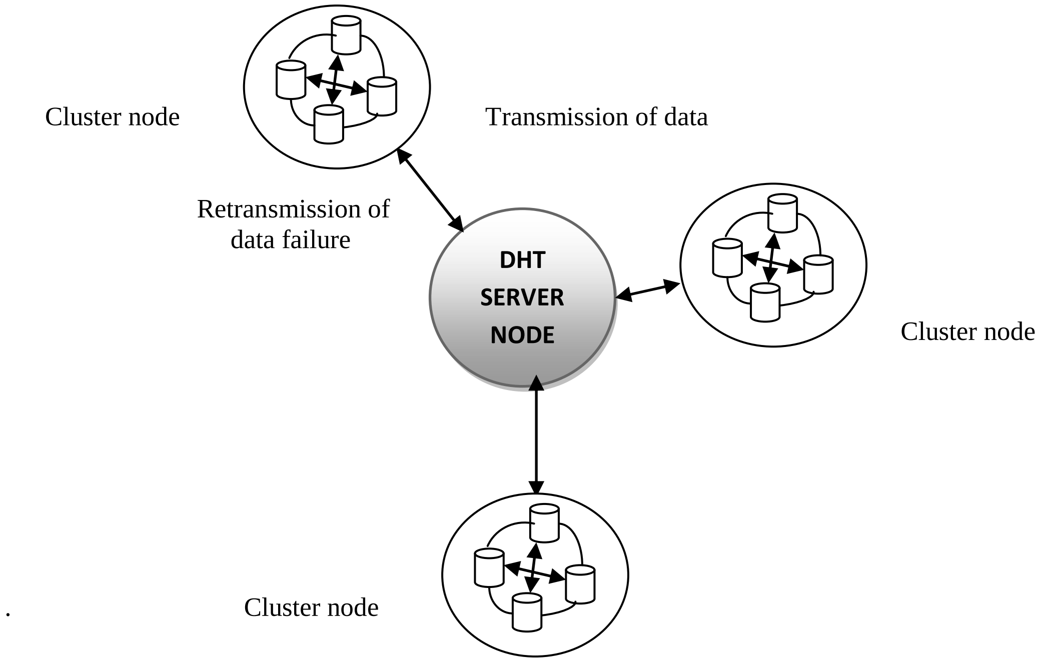

Fig 1 Architecture of Packet Transmission

IV. Conclusion

A Finally most of the sensor node has been transmitted and balanced nodes are which is not transmitted it will redistribute node process and it transfer node using TTL logic. Here protocol consumes almost minimal memory and the simulations show that it outperforms all other detection protocols in terms of communication cost, while the detection probability is satisfactory.

Acknowledgements

The author extends special thanks to the anonymous re viewers for valuable comments here fig 1 shows the group of nodes in form a group of cluster node and transmission of packets and its calculate the node rate and failure packet can retransmitted based on concept of Piggy backing and prefetching concept and for security transmission without forming clone node and secured.

References

[1]. Zhujun li, member; *IEEE,* and Guang Gong, senior member*, IEEE* "On the Node Clone Detection in Wireless Sensor Networks"

Journal Papers:

[2]. G. Anandharaj , Dr.R. Anitha "A Distributed Location Aware Cache Maintenance Technique for Mobile Computing Environments" (Journal of Computational Information Systems 8: 7 (2012) 2839–2849))

Chapters in Books:

[3]. Sunho Lim Soo-Hoan Chae "On Improving The Robustness Of Partitionable Internet-Based Mobile Ad Hoc Networks" (Computing and Informatics, Vol. 30, 2011, 429–446)

Proceedings Papers:

[4]. Jaeyeon Jung, Arthur W. Berger and Hari Balakrishnan "Modeling TTL-based Internet Caches, *Pro"c. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies* (Volume:1)