INTENSIFYING SECURITY IN SERVER LOAD BALANCING IN WSN

Gayathri.V, M.E-CSE, Kayalvizhi.R, M.E-CSE,AP/CSE.

***Abstract*--The increasing demand for content is straining operator's networks, thereby necessitating development of alternative content delivery mechanisms. Distributed caching architectures constitute a promising solution for mitigating the effects of demand growth by placing popular content files in proximity to users, rather than in a central site. The goal is to reduce the server load by serving as many requests as possible by the caches. In the content placement problem in multiple-level hierarchical caching networks where user requests for files are routed upwards toward content servers, satisfied by intermediate. The Hierarchy Aware Content Placement Algorithm for Two-Level Hierarchies solves the content placement problem. The main drawback of existing is FIFO scheduling .In this project, job scheduling algorithm is applied to reduce the server work load by separate the workload by average time. Level based data aggregation algorithm in wireless sensor networks is employed to reduce the communication overhead and prolong the network lifetime. Each node receives the aggregation results from its parent and its siblings and verifies the aggregation result of the parent node. DSP algorithm applied for bandwidth allocation to form a cluster. The techniques are applied to achieving a provably better approximation ratio and reduce the time delay service and improve security.**

***Keyword*—level based data aggregation, cache process, dynamic source protocol.**

I. INTRODUCTION

Wireless sensor networks (WSN) sometimes called as wireless sensor and actuator network (WSAN), are spatially distributed self-directed sensors to monitor physical or environmental conditions. To cooperatively pass their data through the network to a main location.The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

The rapid increase of content delivery over the Internet has led to the proliferation of Content Distribution Networks (CDNs).CDNs operate large numbers of servers that "push" the content of their subscribed clients close to the end-users. In all cases, storage capacity (or memory) is employed to bring valuable information in close proximity to the end-users is called Caching. This Caching strategy provide an effective mechanism for mitigating these massive bandwidth requirements by replicating the most popular content closer to the network edge, rather than storing it in a central site.The reduction in the traffic load lessens the required transport capacity and capital expense, and alleviates performance bottlenecks. The project is to reduce the server load by serving as many requests as possible by the caches. If the system need to improve the more performance, then it would have increase the number of caches. That is, implement the system like hierarchical caching networks. To improve the performance of the network user requests for files are routed upwards toward content servers, satisfied by intermediate nodes if the latter have cached the requested files. It can solve optimal polynomial-time when the caches are installed on a single hierarchy path. For the general case, we develop an algorithm achieving a provably better approximation ratio than the best-known counterparts. A cache is a temporary storage used by wireless network to reduce the average cost (time or energy) to access data from the main storage location.The cache is a smaller, faster memory which stores copies of the data from popular used main memory locations. When the mobile station wants to access the popular file, the cache storage provides that file to mobile station. These reduce the distance between storage to the end user.

Caching is a mature idea from the domains of web caching, content delivery networks, and memory optimization in operating systems. Why is

caching still an active topic of discussion? In the 90s, the traffic in the web exploded, leading its inventor Sir Tim Berners-Lee to declare the network congestion as one of the main challenges for the Internet of the future. The congestion was caused by the dotcom boom and specifically due to the client-server model of connectivity. A cache is a temporary storage used by wireless network to reduce the average cost (time or energy) to access data from the main storage location. The cache is a smaller, faster memory which stores copies of the data from popular used main memory locations. When the mobile station wants to access the popular file, the cache storage provides that file to mobile station. This reduces the distance between storage to the end user. A hierarchical cache concept is only implementing in bottom level of cache. That is, hierarchies involving caches at the leaf nodes only, where the leaf nodes can exchange their cached files in an on-demand manner leading to reduced cumulative content delivery cost. However, installing caches at multiple levels alters the content placement problem in a fundamental way and calls for alternative solution techniques. Motivation question to implement the proposed system is: what the computational complexity of the content placement problem is in multiple-level cache hierarchies and whether additional solutions with improved approximation guarantees are possible. A file of data on a local hard drive. When downloaded data are temporarily stored on the user's local disk or on a local network disk, it speeds up retrieval the next time the user wants that same data (Web page, graphic, etc.) from the Internet or other remote source. See Web cache and cache. The cache (pronounced "cash") is a space in your computer's hard drive and in RAM memory where your browser saves copies of previously visited Web pages. Your browser uses the cache like a short-term memory.

Our technical contributions can be summarized as follows:

a. Problem of data level security.

The content can be transfer from one level to another it can involve to most of attacks and data loss. The secure sharing of secrecy data is storing on the trusted nodes in presence of Level based scheme by users. In the level based scheme that can have proper verification and authentication about the data to be shared. 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.

b. Problem of user level security.

These works use neighborhood 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.

c. Level based data aggregation algorithm.

The level based data aggregation algorithm is a level based scheme in this all the data is being transfer highly secured. Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. The data transfers from the parent node to the child node are being aggregated. In this the purpose of aggregation all the data is should be evaluated and produce a certification for the aggregated data. The data transfer to another level of cache then the node can check the data and the certification from the above aggregation process. So the certificated data only allowed for aggregating. The corrupted data are to be eliminated from the purpose of aggregation.

d. Dynamic source protocol algorithm.

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. A trust-based approach is recommended to minimize the overheads of intruder detection system and detect the abnormal behavior nodes.

II. RELATED WORK.

Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficult to predict mobility patterns, and long feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for node. Since there may be no neighboring nodes at the moment of the misbehavior cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less. In

network, caching is used as an effective technique to achieve scalability, self-organization, power saving, channel 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 caching can also increase network scalability and decrease the cost. Network with the nodes with different energy levels can prolong the network lifetime of the network and also its reliability.

III. PROBLEM STATEMENT.

The content can be transfer from one level to another it can involve to most of attacks and data loss. The secure sharing of secrecy data is storing on the trusted nodes in presence of Level based scheme by users. In the level based scheme that can have proper verification and authentication about the data to be shared. 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 neighborhood 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. The system is not sufficient to provide security the server load of CDN. The end users experience the delay over content delivery. The energy expenditure of the process is not able to reduce. The existing cannot provide a proper authentication and verification. More time consumed in FIFO scheduling. Forged data are causes accuracy degradation. Waste of energy and power. The existing only focus to increase the number of nodes not worried about data accuracy and malicious node attack.

IV. SYSTEM MODEL.

In this section, we introduce the system model and formally define the security problem.

System Model considers a general multiple-level hierarchical network like the one depicted in Figure 1. 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 untruth behaviors which may lead to the exposure of the secrecy data. 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 neighborhoods 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.

It is good chance of bringing the source in contact with destination to nodes. High probability of message delivery to end user. 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. 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. The data rating is updated by a node for its friend on the basis of amount of data it transfers for it. If any node entrusts in the transfer the data, the Dynamic Source Protocol calculates the alternate path. . In the current research, a trust-based approach is recommended to minimize the overheads of intruder detection system and detect the abnormal behavior nodes. The data transfers from the parent node to the child node are being aggregated. In this the purpose of aggregation all the data is should be evaluated and produce a certification for the aggregated data. The data transfer to another level of cache then the node can check the data and the certification from the above aggregation process. So the certificated data only allowed for aggregating. The corrupted data are to be eliminated from the purpose of aggregation. 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 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 behavior 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. The level based schema can provide the process of data aggregation. Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. A common aggregation purpose is to get more information about particular groups based on specific variables such as age, profession, or income.

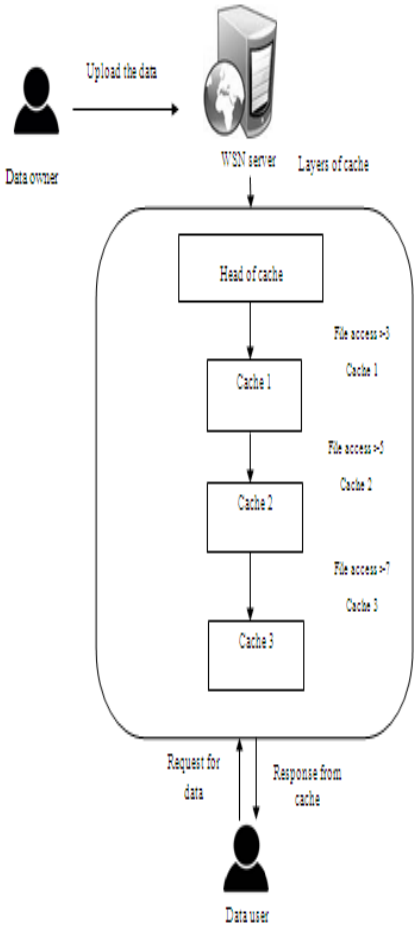

Fig. 1. Graphical illustration of a hierarchical caching network using level based scheme.

In this model can focus mainly on security to reduce the server load of CDN. The benefits of the process is less time to access the file. Malicious nodes can be detected and avoided. The end users experience the fast to deliver the content. The energy expenditure of the process is able to reduce. Confirming authentication by level based scheme. Prolong the network lifetime. Reduce forged data. Providing security from the unauthorized user by abstraction. Increase files accuracy.

V. LEVEL BASED DATA AGGREGATION ALGORITHM.

Typically, there are three types of nodes in WSN: normal sensor nodes, aggregators, and end user. The aggregators collect data from a subset of the network, aggregate the data using a suitable aggregation function and then transmit the aggregated result to an upper aggregator or to the end user who generates the query. The end user is entrusted with the task of processing the received sensor data and derives meaningful information reflecting the events in the target field. It can be the base station or sometimes an external user who has permission to interact with the network depending of the network architecture. Data communication between sensors, aggregators and the end user consumes a large portion of the total energy consumption of the WSN. The WSN in figure 1 contains 16 sensor nodes and uses SUM function to minimize the energy consumption by reducing the number of bits reported to the base station. Node 7, 10-16 are normal nodes that are collecting data and reporting them back to the upper nodes whereas nodes 1-6, 8, 9 are aggregators that perform sensing and aggregating at the same time. In this example 16 packets traveled within the network and only one packet is transmitted to the base station. However, the number of traveling packets would increase to 50 packets if no data aggregation exists. This number of packets has been computed for one query. In the existing data aggregation is performed in the higher level only. But in this process that can be performed in all the level of the cache.The proper certification is produced in a process of data aggregation. This can reduce the amount of data losses. The data transfer to another level of cache then the node can check the data and the certification from the above aggregation process. So the certificated data only allowed for aggregating. The corrupted data are to be eliminated from the purpose of aggregation.

VI. DSP ALGORITHM.

The Dynamic Source protocol (DSP) is a simple and efficient routing protocol designed specifically for use in wireless networks of nodes. DSP allows the network to be completely self-organizing and

self-configuring, without the need for any existing network infrastructure or administration DSP has been implemented by numerous groups, and deployed on several test beds. Networks using the DSP protocol have been connected to the Internet. DSP can interoperate with Mobile IP, and nodes using Mobile IP and DSP have seamlessly migrated between WLANs, cellular data services, and DSP mobile ad hoc networks. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSP to scale automatically to only that needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSP protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSP protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes, and is designed to work well with even very high rates of mobility.

VII. CONCLUSION.

In this paper the result from the comparison of various routing protocols such as First Contact and Direct Delivery. The data transmission between one node 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. Then propose a level based data aggregation algorithm that solves the problem of data degradation in a cluster of caches. survey of data aggregation algorithms in wireless sensor networks. All of them focus on optimizing important performance measures such as network lifetime, data latency, data accuracy and energy consumption. Efficient organization, routing and data aggregation tree construction are the three main focus areas of data aggregation algorithms Level based data aggregation algorithm that achieves a provably better approximation ratio than the best known counterparts. The content popularity distributions are steep and diverse across nodes, and the cache capacities at the upper hierarchy levels are large. This system mostly achieves the cache hit. Because of this the overall system performance is improved.

VIII. FUTURE WORK.

In future the security for WSN can be increased then the control technique for multilevel caching network can be further simplified and generalized to different levels .The levels of multilevel configuration can be increased and further improvements in terms of performance and power quality. Data transmissions, 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] Poularakis .K and Tassiulas .L, “On the Complexity of Optimal Content Placement in Hierarchical Caching Networks” in IEEE, vol. 64, issue. 5, pp. 2092-2103, May 2016.

[2] J. Dai *et al.*, “Collaborative hierarchical caching with dynamic request routing for massive content distribution,” in *Proc. IEEE Infocom*, 2012,pp. 2444–2452.

[3] S. Borst, V. Gupta, and A. Walid, “Distributed caching algorithms for content distribution networks,” in *Proc. IEEE Infocom*, 2010, pp. 1–9.

[4] N. Golrezaei, K. Shanmugam, A. Dimakis, A.Molisch, and G. Caire,“FemtoCaching: Wireless video content delivery through distributed caching helpers,” in *Proc. IEEE Infocom*, 2012, pp. 1107–1115,

[5] K. Poularakis, G. Iosifidis, and L. Tassiulas, “Approximation algorithms for mobile data caching in small cell networks,” *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3665–3677, Oct. 20142001, pp. 661–670.

[6] J. He, H. Zhang, B. Zhao, and S. Rangarajan, “A collaborative framework for in-network video caching in mobile networks,” in *Proc. IEEE Conf. Sensor Mesh Ad Hoc Commun. Netw. (SECON)*, 2013, pp. 406–414.

[7] L. Qiu, V. N. Padmanabhan, and G.M. Voelker, “On the placement of web server replicas,” in *Proc. IEEE Infocom*, 2001, vol. 3, pp. 1587–1596.

[8] N. Laoutaris, V. Zissimopoulos, and I. Stavrakakis, “On the optimization of storage

capacity allocation for content distribution," *Comput. New.*, vol. 47, no. 3, pp. 409–428, 2005.

[9] E. Angel, E. Bampis, G. Pollatos, and V. Zissimopoulos, "Optimal data placement on networks with constant number of clients," *Theor. Comput. Sci.*, vols. 540–541, pp. 82–88, 2014.

[10] M. M. Amble, P. Parag, S. Shakkottai, and L. Ying, "Content-aware caching and traffic management in content distribution networks," in *Proc. IEEE Infocom*, 2011, pp. 2858–2866.