International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 10 Issue 1 –OCTOBER 2014.

Route Maintenance for QOS and Sleep Scheduling Algorithm using Content Delivery Networks

Bhuvaneswari.G[*1], and R.Rameshkumar[#2]

[*] *PG Student, Dept of CSE, Gnanamani College of Technology, Namakkal,India*

[#] *Asst Professor (Computer Science), Gnanamani College of Technology, Namakkal,India*

***Abstract*— The problem of low penetration of multicast and QoS enabling mechanisms in IP networks, overlay network techniques are used that avoid undue duplication of Multimedia streaming flows while transcoding or scalable encoding can be used for graceful adaptation of the stream to the capabilities of access systems. The idea described in this paper is based on a flexible network independent platform which can be easily deployed through the use of personal computers. It employs overlay network solutions for setting up the media distribution scheme, independently from the underlying network. It incorporates mechanisms for dynamic setup and discovery of nodes, adaptability to network conditions and self- configuration, Route Maintenance with help of protocol. The design and implementation in sleep schedule algorithm of the Relay Modules, an essential element in such architecture, is outlined.**

***Keywords*— Content Delivery Networks, self- configuration, Route Maintenance, Qos, sleep schedule algorithm.**

I. INTRODUCTION

Wireless Sensor Networks have emerged as research areas with an overwhelming effect on practical application development. They permit fine grain observation of the ambient environment at an economical cost much lower than currently possible. In hostile environments where human participation may be too dangerous in sensor network which may provide a robust service. Sensor networks are designed to transmit data from an array of sensor nodes to a data repository on a server. The advances in the integration of MEMS, microprocessor and wireless communication technology have been enabled the deployment of large scale. WSN has potential to design many new applications for handling emergency, military and disaster relief operations that requires real time information for efficient coordination and planning.

Sensors are devices that produce a measurable response to a change in a physical condition like temperature, humidity, pressure etc. WSNs may consist of many different types of sensor such as seismic, magnetic, thermal, visual, infrared, and acoustic and radar capable to monitor a wide variety of ambient conditions. Through each individual sensor may have severe resource constraint in terms of energy, memory, communication and computation capabilities; large number of them may collectively monitor the physical world and process the information on the fly environment.

A WSN is different from other popular wireless networks like cellular network, WLAN and Bluetooth in many ways. Compared to other wireless networks, a WSN has much more nodes in a network, distance between the neighbouring nodes is much shorter and application data rate is much lower also. Due to these characteristics, power consumption in a sensor network will be minimized. To keep the cost of the entire sensor network down, cost of each sensor needs to be reduced. It is also important to use tiny sensor nodes. A smaller size makes it easier for a sensor to be embedded in the environment it is in. WSNs may also have a lot of redundant data since multiple sensors can sense similar information. The sensed data therefore need to be aggregated to decrease the number of transmission in the network, reducing bandwidth usage and eliminating unnecessary energy consumption in both transmission and reception.

The main characteristics of a WSN include,

- Power consumption using batteries or energy harvesting
- Ability to cope with node failure
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale deployment
- Ease of use

In a WSN, sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards a sink, which could be a gateway, base station, storage node, or querying user. A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward.

The large-scale deployment of wireless sensor networks (WSNs) and the need for data aggregation necessitate efficient organization of the network topology for the purpose of balancing the load and prolonging the network lifetime. Clustering has proven to be an effective approach for organizing the network into a connected hierarchy. In this article, we highlight the challenges in clustering a WSN, discuss the design rationale of the different clustering approaches, and classify the proposed approaches based on their objectives and design principles. We further discuss several key issues that affect the practical deployment of clustering techniques in sensor network applications.

In order to support data aggregation through efficient network organization, nodes can be partitioned into a number of small groups called clusters. Each cluster has a coordinator, referred to as a cluster head, and a number of member nodes. Clustering results in a two-tier hierarchy in which cluster heads (CHs) form the higher tier while member nodes form the lower tier. The member nodes report their data to the respective CHs. Research on clustering in WSNs has focused on developing centralized and distributed algorithms to compute connected dominating sets. The CHs aggregate the data and send them to the central base through other CHs. Because CHs often transmit data over longer distances, they lose more energy compared to member nodes. The network may be clustered periodically in order to select energy-abundant nodes to serve as CHs, thus distributing the load uniformly on all the nodes. Besides achieving energy efficiency, clustering reduces channel contention and packet collisions, resulting in better network throughput under high load.

H.Chan and A. Perrig., [1] has expect future sensor networks to consist of hundreds or thousands of sensor nodes. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes.

Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks—for example, falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service. Addressing the problem of sensor node compromise requires technological solutions.

V. Bhuse, A. Gupta, and L. Lilien, “Dpdsn., [3] as Denial-of-service (DoS) attacks on wireless sensor networks (WSNs) can deplete network resources and energy without much effort on the part of an adversary. Packet-dropping attacks are one category of DoS attacks. Lightweight solutions to detect such attacks on WSNs are needed. Current techniques for detecting such attacks in ad hoc networks need to monitor every node in the network. Once they detect malicious nodes that drop packets, a new path has to be found that does not include them. In this paper, we propose a lightweight solution called DPDSN. It identifies paths that drop packets by using alternate paths that WSN finds earlier during route discovery. Responding to a packet-dropping attack incurs no additional cost because one of the alternate paths is utilized for the subsequent communication. DPDSN does not require monitoring individual nodes, making it feasible for WSNs. We formulate the probability of success and failure of DPDSN in the presence of malicious nodes that drop packets. We compare our approach with existing techniques. Our analysis found that the overhead ofDPDSN is at most for a two-dimensional grid network on nodes. Our simulations show that the overhead of DPDSN for a WSN with 100 nodes is less than 3% of energy consumed on route discovery when using DSR or Directed Diffusion routing protocols.

R. Roman, J. Zhou, and J. Lopez., [5] Wireless sensor networks (WSNs) are vulnerable to different types of security threats that can degrade the performance of the whole network; that might result in fatal problems like denial of service (DoS) attacks, routing attacks, Sybil attack etc. Key management protocols, authentication protocols and secure routing cannot provide security to WSNs for these types of attacks. Intrusion detection system (IDS) is a solution to this problem. It analyses the network by collecting sufficient amount of data and detects abnormal behaviour of sensor node(s). IDS based security mechanisms proposed for other network paradigms such as ad hoc networks, cannot directly be used in WSNs. Researchers have proposed various intrusion detection systems for wireless sensor networks during the last few years. We classify these approaches into three categories i.e. purely distributed, purely centralized and distributed-centralized. In this paper, we present a survey of these mechanisms. These schemes are further differentiated in the way they perform intrusion detection.

S. Banerjee and S. Khuller., [6] of clustering scheme to create hierarchical control structure in the multi-hop wireless networks has many constraints. A cluster is defined as a subset of vertices, whose induced graph is connected. In addition, a cluster is required to obey certain constraints that are useful for management and scalability of the hierarchy. All these constraints cannot be met simultaneously for general graphs, but we show how such a clustering can be obtained for wireless network topologies. Finally, we present an efficient distributed implementation of our clustering algorithm for a set of wireless nodes to create the set of desired clusters.

K.Ioannis, T.Dimitriou, and F.C.Freiling., [12] is Denial-of-Message Attack (DoM), where sensor nodes are deprived of broadcast messages. While nodes can fail to receive broadcasts due to benign network failures, here we consider the possibility that these failures are maliciously induced by an attacker. A simple approach is for every broadcast recipient to send an authenticated acknowledgment for each broadcast message. However, this approach results in a substantial load

on the network to carry acknowledgments and on the base station to process them.

II. ORGANIZATION OF PAPER

In the WSN, it consists of a system initialization phase and several equal-duration rounds of intruder identification phases. In the initialization phase, sensor nodes form a topology which is a directed acyclic graph (DAG). A routing tree is extracted from the DAG. In each round, data are transferred through the routing tree to the sink. Each packet sender/ forwarder adds a small number of extra bits to the packet and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that must be bad and nodes that are suspiciously bad.

According to the scheme, a dynamic routing tree rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping rate associated with every sensor node, and then run our proposed node categorization algorithm to identify nodes that are droppers/ modifiers for sure or are suspicious droppers/modifiers. As the tree structure dynamically changes every certain time interval, behaviours of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviours has been accumulated, and the sink periodically run our proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. As a certain number of rounds have passed, the sink will have collected information about node behaviours in different routing topologies. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and the nodes' topological relationship. To further identify bad nodes from the potentially large number of suspiciously bad nodes, the sink runs heuristic ranking algorithms.

III. SYSTEM DESIGN

In a WSN, sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node.

Node categorization ensures that the clustering process starts simultaneously throughout the network. Lack of categorization may result in a suboptimal choice of CHs, especially for probabilistic approaches. However, the clustering process can be triggered by nodes with faster clocks. This happens when such nodes start querying their neighbours for updated information in order to start the clustering process. Received queries trigger the clustering process at these neighbours, and these neighbours in turn trigger their neighbours, and so on.

An important objective of any clustering technique is network connectivity. For intra-cluster communication, a cluster member communicates with its CH either directly. Connectivity in this case is a result of the success of cluster formation. For inter-cluster communication, two approaches were adopted in order to maintain connectivity. In one approach, nodes on cluster boundaries are used as gateways to relay data among CHs. This approach is suitable in networks that use a fixed transmission power. Network density has to be sufficiently high in order to ensure that enough gateways are present at the intersection areas between clusters.

To balance the trade-off, we further propose the HR method. According to HR, the node with the highest accused account value is still first chosen as most likely bad node. After a most likely bad node has been chosen, the one has the highest accused account value among the rest is chosen only if the node has not always been accused together with the bad nodes that have been identified already. The accusation account value is considered as an important criterion in identification, and the possibility that an innocent node being framed by bad nodes is also considered by not choosing the nodes who have always being suspected together with already-identified bad node.

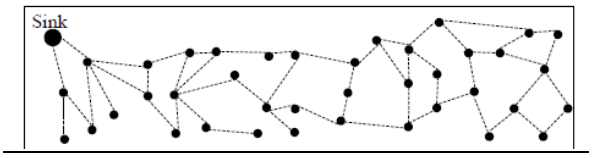

Fig.1: System Model

IV. EXPERIMENTAL EVALUATION

Distributed clustering protocols achieve their best performance when sensor nodes are categorized. Node categorization ensures that the clustering process starts simultaneously throughout the network. Lack of

categorization may result in a suboptimal choice of CHs, especially for probabilistic approaches. However, the clustering process can be triggered by nodes with faster clocks. This happens when such nodes start querying their neighbours for updated information in order to start the clustering process. Received queries trigger the clustering process at these neighbours, and these neighbours in turn trigger their neighbours, and so on. It is not essential that "all" the nodes in the network start the clustering process simultaneously. In fact, it is sufficient that the process starts in different regions simultaneously. Probabilistic techniques that use a number of iterations (e.g., [3, 5]) are therefore less impacted by the lack of synchronization than single-iteration techniques.

If a compromised node modifies the packets that it is supposed to forward, the node can be detected with the fore described scheme. This is because modified packets will be detected by the sink and thus be dropped. This is equivalent to that the packets are dropped by the modifier; hence, the packet modifier can be identified as a packet dropper using the Hybrid Ranking-Based Approach in cluster nodes.

4.1 Sensor Node Deployment

Large number of sensor nodes are randomly deployed in a two dimensional area. Each sensor node generates sensory data periodically and all these nodes collaborate to forward packets containing the data towards a sink. The sink is located within the network. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighbouring nodes right after deployment. The purpose of sensor node deployment is to set up secret pair wise keys between the sink and every regular sensor node, to establish the cluster network and routing algorithm to facilitate packet forwarding from every sensor node to the network.

4.2 Neighbour Distance Calculation

In iterative clustering techniques, a node waits for a specific event to occur or certain nodes to decide their role before making a decision. A node waits for all its neighbours with higher weights to decide to be CHs or join existing clusters. Nodes possessing the highest weights in their one-hop neighbourhoods are elected as CHs

4.3 Cluster Node Formation

To support data aggregation through efficient network organization, nodes can be partitioned into a number of small groups called clusters. Each cluster has a coordinator, referred to as a cluster head, and a number of member nodes. Clustering results in a two-tier hierarchy in which cluster heads (CHs) form the higher tier while member nodes form the lower tier. The member nodes report their data to the respective CHs. The CHs aggregate the data and send them to the central base through other CHs. Because CHs often transmit data over longer distances, they lose more energy compared to member nodes. The network may be reclustered periodically in order to select energy-abundant nodes to serve

4.4 Packet Sending and Forwarding

When a node wants to send out a packet, it attaches to the packet with a sequence number, encrypts the packet only with the key shared with the sink, and then forwards the packet to the cluster head. When an innocent intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of the packet, encrypts the packet, and then forwards the packet to its parent. After receiving a packet, the sink decrypts it, and thus finds out the original sender and the CHs, thus distributing the load uniformly on all the nodes packet sequence number. The sink tracks the sequence numbers of received packets for every node, and for every certain time interval, which we call a round, it calculates the packet dropping ratio for every node. `

4.5 Node Categorization

In this module, to identify nodes those are droppers/modifiers for sure or are suspicious droppers/ modifiers. Behaviours of sensor nodes can be observed in a large variety of scenarios. In every round, for each sensor node, the sink keeps track of the number of packets sent from sensor node, the sequence numbers of these packets, and the number of flips in the sequence numbers of these packets. In the end of each round, the sink calculates the dropping ratio for each sensor node. The dropping ratio in this round is calculated based on the dropping ratio of every sensor node and the cluster based algorithm, the sink identifies the nodes that are droppers for sure and that are possibly droppers.

4.6 Hybrid Ranking Algorithm

The bad node modification is done by HR method to reduce packet droppers and modifiers. The suspiciously bad nodes are identified based on the simultaneous selection of nodes for sending packet. For each of these scenarios, node categorization algorithm is applied to identify sensor nodes that are bad for sure or suspiciously bad. After multiple rounds, sink further identifies bad nodes from those that are suspiciously bad by applying several proposed heuristic methods. The tree used for forwarding data from sensor nodes to the sink is dynamically changed from round to round. In other words, each sensor node may have a different parent node from round to round. We rank the suspiciously bad nodes based on their probabilities of being bad, and identify part of them as most likely bad nodes.

V. CONCLUSION

Here, the simple yet effective scheme to identify misbehaving forwarders that drop and modify packets in the cluster network. The sink recover source of the packet and figure out the dropping ratio associated with each sensor node. Also the node is categorized based on the packet received by the destination. Our packet dropper/modifier identification scheme is implementedin the ns-2 simulator (version 2.3) to evaluate the effectiveness and efficiency of this clustering

node. We measure the performance of our scheme from two aspects: the detection rate, defined as the ratio of successfully identified bad nodes, and the false positive probability, defined as the ratio of adverse innocent nodes over all innocent nodes. Extensive analysis and simulations have been conducted and verified the effectiveness of the proposed scheme in various scenarios. The implementation provides the effective scheme to identify the misbehaving forwarders. The sensor nodes deployment can be set from 5 to 50 numbers randomly. It takes more time for finding the misbehaving nodes, if there is increase in the number of nodes. In each round the sensor node keeps track of the packets send. The dropping ratio is calculated between the source node and the destination node.

VI. REFERENCES

[1] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Computer,October 2003.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," the First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127, May 2003.

[3] V. Bhuse, A. Gupta, and L. Lilien, "Dpdsn: Detection of packet-dropping attacks for wireless sensor networks," In the Trusted Internet Workshop, International Conference on High Performance Computing, December 2005.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," ACM MobiCom, August 2000.

[5] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," Third IEEE Annual Consumer Communications and Networking Conference (CCNC), pp. 640–644, January 2006.

[6] S. Banerjee and S. Khuller, "A Clustering Scheme for Hierarchical Control in MultihopWireless Networks," Proc. IEEE INFOCOM, Apr. 2001, pp. 1028–37.

[7] OssamaYounis, Marwan Krunz, and SrinivasanRamasubramanian, University of Arizona"Node Clustering in Wireless Sensor Networks", Recent Developments and Deployment Challenges.

[8] G. Chen and I. Stojmenovic, Clustering and routing in wireless ad hoc networks, TR-99-05, SITE,University of Ottawa (June 1999).

[9] A Path-Connected-Cluster Wireless Sensor Network and its Formation, Addressing, and Routing Protocols Chia-Hung Tsai and Yu-Chee Tseng, Fellow, IEEE

[10] C.-T.Cheng, C. K. Tse, and F. C. M. Lau. "A Clustering Algorithm for Wireless Sensor Networks Based on Social Insect Colonies", IEEE Sensors Journal, 11(3):711–721, 2011.

[11] M. Ali and Z. A. Uzmi. "An Energy-Efficient Node Address Naming Scheme for Wireless Sensor Networks", In Proc. of IEEE Int'l Networkingand Communications Conference (INCC), 2004.

[12] K.Ioannis, T.Dimitriou, and F.C.Freiling, "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts", In Proc. of IEEE Symp.Security and policy, 2005