International Journal on Applications in Information and Communication Engineering
Volume 5 : Issue 1: May 2019, pp 5 – 10 www.aetsjournal.com ISSN (Online) : 2394 - 6237

AN EFFICIENT RESPONSIBLE DATA COLLECTION METHODOLOGY IN SENSOR-CLOUD SYSTEMS

S.RENUGADEVI , V.KARTHI

Abstract— Wireless Sensor Cloud Network is an important tool for monitoring physical phenomena in the modern world. The nodes ability to communicate wirelessly removes the need for long wires and enables them to be distributed in an ad-hoc manner wherever and whenever required. One of the main challenges in these cloud CSNs (CWSCNs) is the routing protocol, which aims to transport the data generated by the sensors to the sink. A constantly changing topology means that a fixed path from a sensor to the sink cannot be guaranteed. The more demanding applications also require the consistent delivery of real-time data in highly cloud scenarios.Robust Ad-hoc Sensor Routing (RASeR) protocol is designed to be a reliable solution, even with the high frequency topology changes of a cloud network. It uses a simple hop-count gradient to allow sensor nodes to blindly forward data towards a single sink. A key issue with this type of routing is in keeping the gradient metric up to date, for this reason RASeR uses a design that combines a global time division multiple access (GTDMA) medium access control (MAC) scheme with the routing protocol.In proposed work, the communication in Wireless Cloud Sensor Network (WCSN) is based on mutual trust between the participating nodes. Due to features of open medium, dynamic changing topology, lack of centralized monitoring and management, Mobile Sensor cloud Network (MSCNs) are vulnerable to various security attacks.

I. INTRODUCTION

Wireless sensor cloud Network have recently come into prominence because they hold the potential to revolutionize many segments of our economy and life, from environmental monitoring and conservation, to manufacturing and business asset management, to automation in the transportation and health care industries. The design, implementation, and operation of a sensor network requires the confluence of many disciplines, including signal processing, networking and protocols, embedded systems, information management and distributed algorithms. Such cloud Network are often deployed in resource-constrained environments, for instance with battery operated nodes running un-tethered.

These constraints dictate that sensor network problems are best approached in a hostile manner, by jointly considering the physical, networking, and application layers and making major design tradeoffs across the layers. Advances in wireless networking, micro-fabrication and integration (for examples, sensors and actuators manufactured using micro-electromechanical system technology, or MEMS), and embedded microprocessors have enabled a new generation of massive-scale sensor cloud Network suitable for a range of commercial and military applications.

Un-tethered and has a microprocessor and a small amount of memory for signal processing and task scheduling. Each node is equipped with one or more sensing devices such as acoustic microphone arrays, video or still cameras, infrared (IR), seismic, or magnetic sensors. Each sensor node communicates wirelessly with a few other local nodes within its radio communication range.

Sensor cloud Network extends the existing Internet deep into the physical environment. The resulting new network is orders of magnitude more expansive and dynamic than the current TCP/IP cloud Network and is creating entirely new types of traffic that are quite different from what one finds on the Internet now. Information collected by and transmitted on a sensor network describes conditions of physical environments for example, temperature, humidity, or vibration and requires advanced query interfaces and search engines Sensor cloud Network may inter-network with an IP core network via a number of gateways. A gateway routes user queries or commands to appropriate nodes in a sensor network. It also routes sensor data, at times aggregated and summarized, to users who have requested it or are expected to utilize the information. A data repository or storage service may be present at the gateway, in addition to data logging at each sensor. The repository may serve as an intermediary between users and sensors, providing a persistent data storage. It is well known that communicating 1 bit over the wireless medium at short ranges consumes far more energy than processing that bit.

Ms.S.Renugadevi , Department of Computer Science and Engineering , J.K.K .Nattraja College Of Engineering And Technology , Kumarapalayam.
(Email ID : redrose.devi8@gmail.com)
Mr.V.Karthi , M.E., Assistant Professor , Department of Computer Science and Engineering , J.K.K. Nattraja College Of Engineering And Technology , Kumarapalayam.
(Email ID : karthi10013@gmail.com)

Wireless sensor cloud Network is a trend of the past few years, and they involve deploying a large number of small nodes. The nodes then sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes are great for deployment in hostile environments or over large geographical areas. The sensor nodes leverage the strength of collaborative efforts to provide higher quality sensing in time and space as compared to traditional stationary sensors, which are deployed in the following two ways:

- Sensors can be positioned far from the actual phenomenon, i.e. something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.
- Several sensors that perform only sensing can be deployed. The position of the sensors and communications topology is carefully engineered. They transmit time series of the sensed phenomenon to central nodes.

II. OBJECTIVES

- Mobile Sensor Cloud (MSC) is being cost-effective and quick to install, find many applications in military environments, emergency and rescue operations, civilian environments and education.
- Many researchers have come up with many routing protocols in MSC, as described.
- In these applications data have significant role.But, MSCs are often vulnerable to security attacks that lead to unauthorized access disclosure, disruption, modification.

III. REVIEW OF LITERATURE SURVEY

1) "VEHICLE-BASED SENSOR CLOUD NETWORK FOR TRAFFIC MONITORING"

In this paper, they are interested in understanding what performance for traffic monitoring would be if these sensor cloud Network only provide sparse and incomplete real-time information .The vehicle-based sensor cloud Network have an advantage of cost saving than the traditional stationary sensors, such as loop detectors, and/or video cameras, which lead to high cost of infrastructure and maintenance.This paper is not concerned with details of the networking aspect, but primarily with data processing for traffic monitoring.

This is a fundamental problem need to be solved. Overall, available sensor data are only a byproduct of taxi companies, not designed specifically for traffic monitoring.They carried out a performance evaluation study in urban area of Shanghai by utilizing the sensors installed in about 4000 taxis.Sensors can provide longitude and latitude coordinates, timestamp, etc.

2) "SENSOR CLOUD NETWORK FOR EMERGENCY RESPONSE: CHALLENGERS AND OPPORTUNITIES"

Sensor cloud Network, a new class of devices, has the potential to revolutionize the capture, processing, and communication of critical data for use by first responders.Sensor cloud Network consist of small, low-power, and low-cost devices with limited computational and wireless communication capabilities. They represent the next step in wireless communication's miniaturization, and their power and size make it feasible to embed them into wearable vital sign monitors, location-tracking tags in buildings, and first responder uniform gear.

Sensor nodes' extreme resource limitations represent new challenges in protocol design, application development, and security models. The authors developed CodeBlue a common software infrastructure, to address these challenges. CodeBlue integrates sensor nodes and other wireless devices into a disaster response setting and provides facilities for ad hoc network formation, resource naming and discovery, security and in network aggregation of sensor-produced data.They designed CodeBlue for rapidly changing.

3) "ACHIEVABLE PERFORMANCE IMPROVEMENTS PROVIDED BY ROUTE DISCOVERY IN MULTIHOP WIRELESS CLOUD NETWORK"

When considering many paths in a multi-hop wireless setting, the variability of channels results in some paths providing better performance than other paths, i.e., path diversity.While it is well known that some paths are better than others, a significant number of routing protocols do not focus on selecting the optimal path. However cooperative diversity an area of recent interest, provides techniques to exploit path and channel diversity.Here they examine the potential performance improvement when optimal paths are used. Three settings are examined, where the path loss can be neglected, where path loss is considered but channel correlation is not accounted for and where path loss and channel correlation are accounted for. It is shown that path diversity can lead to dramatic improvements in performance. For example, it is shown that in a 5-hop cloud Network, improvements by of 10-100 are not uncommon and can reach a maximum of a factor of 2000 as the node density grows to infinity. An interesting feature of path diversity is that when fully exploited, paths with more hops provide better

performance than those with fewer hops. It is shown that such behavior occurs when a particular map has a non-zero fixed point.

4) "ROUTING TECHNIQUES IN WIRELESS SENSOR CLOUD NETWORK: A SURVEY"

Wireless Sensor Cloud Network (WSCNs) consist of small nodes with sensing, computation, and wireless communications capabilities.Many routing, power management, and data dissemination protocols have been specifically designed for WSCNs where energy awareness is an essential design issue.The focus, however, has been given to the routing protocols which might differ depending on the application and network architecture. In this paper they present a survey of the state-of-the-art routing techniques in WSCNs.They first outline the design challenges for routing protocols in WSCNs followed by a comprehensive survey of different routing techniques.

5) "ROBUST COOPERATIVE ROUTING PROTOCOL IN WIRELESS SENSOR CLOUD NETWORK"

In wireless sensor cloud Network, path breakage occurs frequently due to node mobility, node failure, and channel impairments.It is challenging to combat path breakage with minimal control overhead, while adapting to rapid topological changes.Due to the Wireless Broadcast Advantage (WBA), all nodes inside the transmission range of a single transmitting node may receive the packet, hence naturally they can serve as cooperative caching and backup nodes if the intended receiver fails to receive the packet. In this paper they present a distributed robust routing protocol in which nodes work cooperatively to enhance the robustness of routing against path breakage.They compare the energy efficiency of cooperative routing with non cooperative routing and show that their robust routing protocol can significantly improve robustness while achieving considerable energy efficiency.

IV. PROPOSED SYSTEM:

Trust embedded AODV (T-AODV) and its trust model, proposed counter attacks selfish nodes in MWSCN. In this, trust evaluation of a node is based on confidence level and forwarding ratio. Forwarding ratio of a node is the ratio of actually forwarded upon requested for forward, and the forwarding ratio weighted by packet size is considered as confidence level. The received forwarding ratio and confidence level from the neighbors contribute towards overall trust evaluation on a node. The T-AODV includes this trust in its rebroadcasted RREQ packets to counter attack malicious nodes in the MSC. It does not allow any intermediate node to send route reply. The scheme presented in WSCN is based on incentives and penalties depending on the node behavior. In this, route trust is computed as the ratio of the number of packets received at the destination to the number of packets forwarded by a node on that route. Node trust is computed based on the difference between observed route trust value and advertised route trust value.

A. METHODOLOGY

- ❖ Raser protocol
- ❖ Add node
- ❖ Route discovery
- ❖ Evaluate trustworthiness of local repaired path
- ❖ Admission of new node
- ❖ View nodes and path

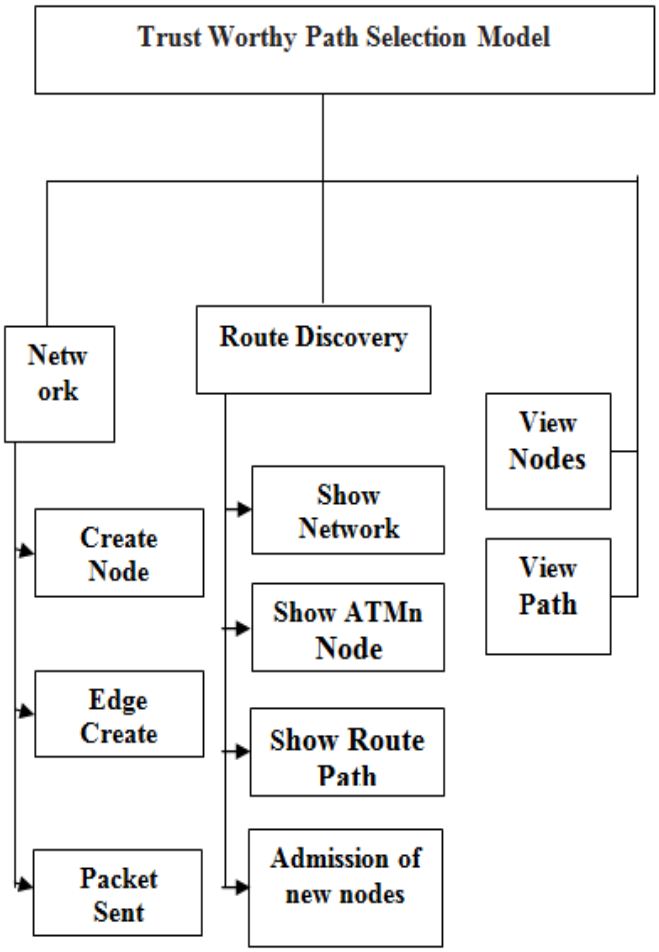
B. ADVANTAGES

- ❖ The proposed system shows that EAODV1, EAODV2 and AAODV are very simple techniques and require substantially less knowledge of the network.
- ❖ Depending on the nature of movement of the nodes the new system can select EAODV1, EAODV2 or AAODV.
- ❖ It is suitable for highly scalable and dynamic cloud Network as it has drastically reduced the amount of overhead.

C. APPLICATION

- ❖ RASeRs adaptability to different scenarios.
- ❖ Reduces power consumption by introducing sleep cycles.
- ❖ Important part of the protocol is the energy saving mechanism.

V. BLOCK DIAGRAM



1) RASER PROTOCOL

The use of diversity packets is designed to increase the route diversity of the protocol without impeding the delay times of the priority packets. So, the diversity packets will increase the number of paths a piece of data may take to the sink, but priority packets will always be transmitted first. Based on this, the oldest priority packets in the queue will be transmitted first, followed by the diversity packets; this is known as normal mode.

- If the node's hop-count is lower than that in the received packet, then the packet should be forwarded with the same priority as it was received.
- If the node's hop-count is higher than that in the received packet, then the packet should be dropped regardless of its priority.
- If the node's hop-count is the same as that in the received packet and the packet has priority status, then the packet should be forwarded with diversity status.
- If the node's hop-count is the same as that in the received packet and the packet has diversity status, then the packet should be dropped.

2) ADD NODE

In this module, the node details are added so that the network can be drawn in route discovery process. The node contains id, isSource node, isATMn node and isDestination node details. All the nodes can be viewed in nodes list.

3) ROUTE DISCOVERY

In this module, a network communication of 'n' nodes say '10' nodes is taken. (This may be any number of nodes). For the given source node, the associated trusted node is found out. Node with more Path trustworthiness is treated as ATMn (Associated Trust Cloud Node). Through that node, the Route request message is passed.

After the route is found out as per the algorithm, during the process of sending/forwarding the RREP message, everyCloud Node in the reverse path broadcasts trust request (TREQ) message, shouting for trust value of the nexthop Cloud Node in the upstream from its neighbors (in Fig. 1(b)). The broadcast is only to one-hop Cloud Nodes.

4) EVALUATE TRUST WORTHINESS OF LOCAL REPAIRED PATH

In this module, when a link break occurs in an active route, the node upstream of that break chooses to repair the link locally if it is closer to the destination. To repair the link break, the repairing node broadcasts a RREQ message for the destination. Since such RREQ message is in response to local link repair, it does not warrant being through ATMn of the repairing node.

If the repairing node receives a RREP then the route is locally repaired, otherwise it transmits a route error (RERR) message to its precursors. When the source node receives the RERR message the source node rediscovers the route. trustworthiness of the locally repaired path are evaluated even if packet drops at the Cloud Node that initiates local repair.

5) ADMISSION OF NEW NODES

In this module, operation is carried out for New Cloud Nodes, joining the network, which are waiting for DELETE PERIOD before transmitting any route discovery messages. During the DELETE PERIOD, new Cloud Nodes receiving control packets create route entries but do not forward any control packets.

Further, during the same, the new Cloud Nodes build their node trust table from their monitored traffic. Based on the trust values in the node trust table, a new Cloud Node gets associated with one of the TdMNs with the highest node trust value.

6) VIEW NODES AND PATH

In this module, all the nodes details are viewed. In addition, the route discovered details are also viewed. Path contains node id, 'n' node in the path and the description details such as the node is source, ATMn, intermediate nodes or the destination node.

VI. INPUT DESIGN

Input design is the process of converting user-originated inputs to a computer understandable format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. A large number of problems with a system can usually be tracked backs to fault input design and method. Every moment of input design should be analyzed and designed with utmost care.

The system takes input from the users, processes it and produces an output. Input design is link that ties the information system into the world of its users. The system should be user-friendly to gain appropriate information to the user. The decisions made during the input design are

- To provide cost effective method of input.
- To achieve the highest possible level of accuracy.
- To ensure that the input is understand by the user.

System analysis decide the following input design details like, what data to input, what medium to use, how the data should be arranged or coded, data items and transactions needing validations to detect errors and at last the dialogue to guide user in providing input.Input data of a system may not be necessarily is raw data captured in the system from scratch. These can also be the output of another system or subsystem. The design of input covers all the phases of input from the creation of initial data to actual entering of the data to the system for processing. The design of inputs involves identifying the data needed, specifying the characteristics of each data item, capturing and preparing data fro computer processing and ensuring correctness of data.

Any Ambiguity in input leads to a total fault in output. The goal of designing the input data is to make data entry as easy and error free as possible. The following forms are used for the input

- **ADD NODE**
- **ROUTE DISCOVERY**
- **SHOW NETWORK**
- **SET ATMn**
- **ROUTE REQUEST (RREQ)**
- **ROUTE REPLY(RREP)AND TRUST REQUEST (TREQ)**
- **TRUST REPLY(TREP)**
- **TRUST EVALUATE (TEVAL)**

1) ADD NODE

In this form, the node details are added so that the network can be drawn in route discovery process. The node contains id, isSource node, isATMn node and isDestination node details. All the nodes can be viewed in nodes list.

2) ROUTE DISCOVERY - SHOW NETWORK

In this form, a network is 'n' nodes is drawn and given as input for the algorithm process. The first node is taken as 'Source Node' and last node is taken as 'Destination Node'.

3) SET ATMn

The Node with ID '2', '3' or '4' which is immediate right node is taken as ATMn Node. Then Route discovery process continues. For sake of convenience, the node with ID '2' or '4' is randomly chosen as ATMn node.

4) ROUTE REQUEST (RREQ)

All neighbors of the ATMn are calculated through algorithm step and further forwarding the RREQ message to their neighbors is carried on, until either the destination or an intermediate Cloud Node with a fresh route to the destination and path trustworthiness above PATH THRESHOLD is reached.

5) ROUTE REPLY (RREP) AND TRUST REQUEST (TREQ)

During the process of sending/forwarding the RREP message, every Cloud Node in the reverse path broadcasts trust request (TREQ) message, shouting for trust value of the nexthop Cloud Node in the upstream from its neighbors. The broadcast is only to one-hop Cloud Nodes.

6) TRUST REPLY (TREP)

Upon receipt of TREQ message, the neighbors broadcast trust reply (TREP) message with trust value of the upstream Cloud Node in their respective node trust table. The broadcast is only to one-hop Cloud Nodes.

7) TRUST EVALUATE (TEVAL)

In order to evaluate the trustworthiness of the discovered path, the ATMn of the source Cloud Node

unicasts trust evaluate (TEVAL) message to the destination with a FLAG set. The FLAG is set to ensure that its acknowledgment is only from the destination node.

8) OUTPUT DESIGN

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application.

The output is designed in such a way that it is attractive, convenient and informative. Forms are designed in Java with various features, which make the console output more pleasing.

As the outputs are the most important sources of information to the users, better design should improve the system's relationships with user and also will help in decision-making. Form design elaborates the way output is presented and the layout available for capturing information.

- **View network node**
- **View ATMN Node**
- **View Path**

A. VIEW NETWORK NODES

Using System.Drawing.Graphics class, in a Panel 'n' number of nodes are drawn with label controls as Nodes. The Labels' text property is assigned with Node Id. The Source Node 'First Label' and Destintion Node 'Last Label' is drawn with green backcolor.

B. VIEW ATMn NODE

After the ATMn node is found out, the node is highlighted as red color label. The node is randomly chosen. Any one of the right nodes immediate to the source node is treated as ATMn node. It is assumed that the node is having more path trustworthiness.

C. VIEW PATH

An arrow is drawn from source node to ATMn node. All other nodes that involve in the path will be drawn with arrows in different color to specify the request routes and reply route.

VII. CONCLUSION

In cloud ad hoc cloud Network (MSCs), each node works not only for itself but also for other nodes. Under such environment, some nodes may misbehave for individual interests. So reputation and trust are instrumental to deal with such misbehaving nodes. Further, in an application perspective MSCs, they are equally prone to security threats as that are in wireline cloud Network.

In this thesis, the proposed solution has not only made the feasibility for placement of firewalls to thwart security threats that are common to wireline cloud Network, but also exploited dynamic and cooperative features of MSCs to deal with misbehaving nodes in discovering trustworthy path.

References

[1] X. Li, et al., Performance evaluation of vehicle-based cloud sensor cloud Network for traffic monitoring, IEEE Trans.Veh.Technol.58(4) (2009) 1647–1653.
[2] D. Ni. Determining traffic-flow characteristics by definition for application in ITS. IEEE Trans on ITS, 2007.
[3] Y. Cho. Estimating velocity fields on a freeway from lower solution videos. IEEE Trans on ITS, v 7, n 4, pp. 463-469,2007.
[4] K. Lorincz, et al., Sensor cloud Network for emergency response : challenges and opportunities, IEEE PervasiveComput.3(4) (2004) 16–23.
[5] S. Bohacek, Performance improvements provided by route diversity in multihop wireless cloud Network, IEEE Trans.CloudComput.7(3) (Mar. 2008)372–384.
[6] P. Sambasivam, A. Murthy, and E. M. Belding-Royer, "Dynamically adaptive multipath routing based on AODV," in MedHocNet, 2004.
[7] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," tech. rep., SUNY - Stony Brook, 2003.
[8] A. Nasipuri and S. R. Das, "On-demand multipath routing for cloud ad hoc cloud Network," in Proceedings of IEEE International Confernce on Computer Communications and Cloud Network ICCCN, pp. 64–70, 1999.
[9] S.-J. Lee and M. Gerla, "AODV-BR: backup routing in ad hoc cloud Network," in IEEE WCNC, pp. 1311–1316, 2000.
[10] L. Zhang, Z. Zhao, Y. Shu, L. Wang, and O. W. Yang, "Load balancing of multipath source routing in ad hoc cloud Network," in Proceedings of IEEE ICC'02, 2002.