ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things

[1]Mrs. C. Navamani M.C.A., M.Phil., M.E., Assistant Professor,
[2]Mr.R.Jayakumar Final MCA.,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: navamanimca@gmail.com, jayakumar15cal16@gmail.com

Abstract- **In this project implement the backpressure scheduling scheme applied in Internet of Things, which can control the network congestion effectively and increase the network throughput. However, in large-scale Emergency Internet of Things (EIoT), emergency packets may exist because of the urgent events or situations. The traditional backpressure scheduling scheme will explore all the possible routes between the source and destination nodes that cause a superfluous long path for packets. Therefore, the end-to-end delay increases and the real-time performance of emergency packets cannot be guaranteed. In existing system, backpressure queue model with emergency packets is first devised based on the analysis of the arrival process of different packets. Meanwhile, EABS combines the shortest path with backpressure scheme in the process of next hop node selecting. The emergency packets are forwarded in the shortest path and avoid the network congestion according to the queue backlog difference. The extensive experiment results verify that EABS can reduce the average end-to-end delay and increase the average forwarding percentage. In proposed system, buffer dimensioning is therefore essential to design a practical and efficient hierarchical clustering algorithm Delay-Tolerant Network(DTN).This project addresses the problem of quantifying the buffer size of DTN source nodes, under replication based routing protocol, using large deviation techniques. The proposed dimensioned-buffer model is shodown to exhibit a routing performance of an equivalent infinite buffer model. In addition, the problem of routing in intermittently connected wireless networks comprising multiple classes of nodes is addressed. The proposed solution perform well in homogeneous scenarios, are not as competent in this setting.**

Index terms– Emergency Internet of things, backpressureScheduling, Event-awareness, network throughput.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless Sensor Networks (WSNs) is currently receiving significant attention due to their unlimited potential. However, it is still very early in the lifetime of such systems and many research challenges exist.

A. Problem Statement

The WSNs are assumed to consist of a large number of sensor nodes. Assuming that, each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. Security Server (SS) is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes.

The proposed scheme considers two types of attacks launched by the adversaries: passive and active attack. Passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis. Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages. In addition, the scheme can also provide message source privacy. Also multiple base station environments are considered.

II.RELATED WORKS

Fan Ye, Haiyun Luo et al describes a large-scale sensor network individual sensors are subject to security compromises. A compromised node can inject into the network large quantities of bogus sensing reports which, if undetected, would be forwarded to the data collection point (i.e. the sink). Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network. In this paper they present a Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. SEF requires that each sensing report be validated by multiple keyed Message Authentication Codes (MACs), each generated by a node that detects the same event. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to dtermine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes. Their analysis and simulations show that, with an overhead of 14 bytes per report, SEF is able to drop 80-90% injected false reports by a compromised node within 10 forwarding hops, and reduce energy consumption by 50% or more in many cases

*Sencun Zhu1, Sanjeev Setia1, Peng Ning*stated Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects false data into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. Standard authentication mechanisms cannot prevent this at-tack if the adversary has compromised one or a small number of sensor nodes. In this paper, they present an interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised. Further, Their scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes. They show that in the worst case B is O(t2).They also propose a variant of this scheme which guarantees B = 0 and works for a small through performance analysis, they show that their scheme is efficient with respect to the security it provides, and it also allows a tradeoff between security and performance. Consider a military application of sensor networks for reconnaissance of the opposing forces, suppose they want to monitor the activities of the opposing forces, e.g., tank movements, ship arrivals or departures, and other relevant events. To control the sensors and collect data reported by the sensors.

Wensheng Zhang, Nalin Subramanian, Guiling Wang explained Numerous authentication schemes have been proposed in the past for protecting communication authenticity and integrity in wireless sensor networks. Most of them however have following limitations: high computation or communication overhead, no resilience to a large number of node compromises, delayed authentication, lack of scalability, etc. To address these issues, they propose in this paper [44]a novel message authentication approach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience to a large number of node compromises, immediate authentication, scalability, and non-repudiation.

Extensive analysis and experiments have also been conducted to evaluate the scheme in terms of security properties and system overhead.John A. Stankovic described Many technical communities are vigorously pursuing research topics that contribute to the Internet of Things (IoT). Today, as sensing, actuation, communication, and control become ever more sophisticated and ubiquitous, there is significant overlap in these communities, sometimes from slightly different perspectives. More cooperation between communities is encouraged. To provide a basis for discussing open research problems in IoT, a vision for how IoT could change the world in the distant future is first presented.

The spectrum of research required to achieve IoT at the scale envisioned above requires significant research along many directions. In this section problems and required
research are highlighted in 8 topic areas: massive scaling, architecture and dependencies, creating

knowledge and big data, robustness, openness, security, privacy, and human-inthe-loop.

AbhijeetBhorkar et al consider the problem of routing packets across a multi-hop network consisting of multiple sources of traffic and wireless links while ensuring bounded expected delay. Each packet transmission can be overheard by a random subset of receiver nodes among which the next relay is selected opportunistically. The main challenge in the design of minimum-delay routing policies is balancing the trade-off between routing the packets along the shortest paths to the destination and distributing the traffic according to the maximum backpressure. Combining important aspects of shortest path and backpressure routing, this paper provides a systematic development of a distributed opportunistic routing policy with congestion diversity (D-ORCD). D-ORCD uses a measure of draining time to opportunistically identify and route packets along the paths with an expected low overall congestion.

D-ORCD with single destination is proved to ensure a bounded expected delay for all networks and under any admissible traffic, so long as the rate of computations is sufficiently fast relative to traffic statistics. Furthermore, this paper proposes a practical

Implementation of D-ORCD which empirically optimizes critical algorithm parameters and their effects on delay as well as protocol overhead.

III.SYSTEM METHODOLOGY

The system presents the buffer dimensioning framework for the replication-based routing protocol. Here, the source node makes replica of the message to any relay node it meets. Based on the replication strategy adapted by the relay nodes, various routing protocols are conceived. Some of them are as follows: i) when the relay nodes also replicate messages among themselves, then the corresponding protocol is called epidemic routing, and ii) when the relay nodes resort to direct transmission forwarding scheme, then the corresponding routing protocol is called two-hop routing protocol.

No relay node scenario is carried out in which the source node needs to meet the destination node to offload the message. In ‘With relay node’ scenario, multi-copy replication-based routing is incorporated. The source node creates a replica of the incoming message to any non-destination nodes it meets.

IV.PROPOSED METHODOLOGY

The proposed system presents a model which is realistic for some practical Network model and with which multilevel clustering can be performed to build a hierarchical network.

Based on this model, the first hierarchical network is being built in which the time-varying nature of the physical topology is reflected by the time-variant information (the contact information) maintained by the links in the hierarchical network. A hierarchical routing algorithm based on the hierarchical network is devised. In this algorithm, the size of per node information is small and scalable.

The proposed system contains all existing system implementation. Also, it contains options for qualified neighbor node detection in worst case scenario. A slicing based approach is selected to filter the neighbor nodes through which the next hop transmission occurs. In addition, all the concepts are implemented unlike existing system where only theoretical discussions are provided.

ExsetupPer mentalServer

In this process, packet type addition, router metric information such as packet type, incoming bit rate, max packet time to live, packet resend times. The incoming packet receiving, sending out normally or adding in queue, dropping from queue or normal sent out are calculated and continuous packet drop is found and alerted to high speed applications to reduce the packet sending speed.

CLIENT APPLICATION

The IP address of the running node is found out and used throughout the coding. The packets are generated and sent out so that the information is stored in a table directly from that node. A new record is ‘PacketsIn’ table is added during application load and packet count is updated each time the packets are sent. A record is inserted in ‘Log’ table with status ‘On’ and ‘Off’ during load and unload. The IP address of the running node is found out and used through out the coding. The packets are generated and sent out so that the information is stored in a table with Port Type field set to ‘S’ directly from that node. A new record is ‘PacketsIn’ table is added during application load and packet count is updated each time the packets are sent. A record is inserted in ‘Log’ table with status ‘On’ and ‘Off’ during load and unload.

ADD ACCESS POINT

In this module, the access point node id, name, IP address details are added and saved in 'AP' table.

ADD MOBILE NODES

In this module, the mobile node id, name, IP address and the initial location details are added and saved in 'Nodes' table.

ASSIGN ACCESS POINT/MOBILE NODES

In this module, the mobile node is assigned with its nearest access point. The details are fetched from 'AP' and 'Nodes' table and saved in 'APNodes' table.

SHOW NETWORK

In this module, the Access Point and nodes are displayed with their current assigned details. The records are fetched from 'AP' and 'Nodes' table.

SELECT SOURCE NODE

In this module, the Source mobile node is selected from 'Nodes' List. The records are fetched from 'Nodes' table.

QOS-ORIENTED DISTRIBUTED ROUTING PROTOCOL (QOD)

This module enhances the QoS support capability of hybrid networks. Taking advantage of fewer transmission hops and anycast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. QOD incorporates five algorithms:

- QoS-guaranteed neighbor selection algorithm to meet the transmission delay requirement
- Distributed packet scheduling algorithm to further reduce transmission delay,
- Mobility-based segment resizing algorithm that adaptively adjusts segment size according to node mobility in order to reduce transmission time.
- Traffic redundant elimination algorithm to increase the transmission throughput.
- Data redundancy elimination-based transmission algorithm to eliminate the redundant data to further improve the transmission QoS. The algorithm for above processes is listed below.

Algorithm 1.Pseudocode for the QOD routing protocol executed by a source node.

if receive a packet forwarding request from a source node then

f this. SpaceUtility< threshold then

Reply to the source node.

end if

end if

if receive forwarding request replies for neighbor nodes then

Determine the packet size Sp(i) to each neighbor I based on Equation (3).

Estimate the queuing delay Tw for the packet for each neighbor based on Equation (2).

Determine the qualified neighbors that can satisfy the deadline requirements based on Tw

Sort the qualified nodes in descending order of Tw

Allocate workload rate Ai for each node based on Equation (1).

for each intermediate node ni in the sorted list do

Send packets to ni with transmission interval Sp(i)/ Ai.

end for

end if

RESULTS AND DISCUSSION

- The proposed GECC Scheme is providing better result to compare the ECC scheme in the authentication mechanism and in the proposed scheme, the verifying time is about half of the authentication generation time, and the generation time is shorter than the verification time.

- Memory utilization of the GECC Scheme is very low comparing to the existing ECC Scheme. The GECC Scheme consumes up to 30 % of memory.

- GECC Scheme provides the efficient energy cost. It provides 25% of cost will be reduced than the existing ECC scheme.

- This GECC scheme doesn't have the threshold problem, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken.

V.CONCLUSION

In this study, proposed a novel event-aware backpressure scheduling scheme to enhance the real-time performance of emergency packets for EIoT. In particular, we first designed a backpressure-based queue model according to the arrival process of different packets that reduces the waiting time of emergency packets in queues. Furthermore, we combine the shortest path method with backpressure scheme to select the next-hop node, which reduces the transmission delay of emergency packets. Finally, the performance of EABS is evaluated. In addition, a Multi hop-based node message sending and compromise detection scheme is proposed using the Global Elliptic Curve Cryptography (GECC). Furthermore, several possible attacks are described against the proposed scheme and proposed multi hop based measures against these attacks. The scheme is evaluated in simulation under various scenarios.

In future, the scheme may evaluate against various types of attacker models. It is believed that a game theoretic model is suited for this evaluation. A variety of strategies may be studied that may be taken by detector and adversary.

REFERENCES

[1] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," IEEE Symposium on Security and Privacy, May 2000.

[2] A. Fiat and A. Shamir. How to Prove Yourself: practical solutions of identification and signature problems. In A. M. Odlyzko, editor, Advances in Cryptology Proceedings of CRYPTO '86, volume 263.

[3] Baeza-Yates.R, and Ribeiro-Neto.B, "Modern Information Retrieval". Addison-Wesley, June 1999.

[4] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards.In G. Brassard, editor, Advances in Cryptology.

[5] Cristianini N. and Shawe-Taylor J., An Introduction to Support Vector Machines and Other Kernel-based Learning Methods, Cambridge University Press, 2000.

[6] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In Advances in Cryptology CRYPTO 92, LNCS 740, pages 471486, 1993.

[7] C. K. Won and S. S. Lam, "Digital signatures for flows and multicasts," IEEE ICNP, 1999.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Sig-natures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[9] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.