INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Integrated Collective Node Behavior Analysis with Onion Protocol for Best & Secured Data Transmission

V. Ohm Sri Eswar
eswar.kishna@gmail.com
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu

Albert
eswar.kishna@gmail.com
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu

Ankayarkanni B
ankayarkanni.s@gmail.com
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu

B Vinil
vinilbysani143@gmail.com
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

Now-a-days communication from one place to another and transfer of data over the network has become an important part of our day to day life. Hence in order to make safe and secured data transmission in this communication process and to provide security to the data sent 'Onion Protocol' is used. Over here integrated collective node behavior analysis is done with Onion Protocol for best and secured data transmission. In Onion routing technique the sender and receiver remain anonymous. The sender remains unknown and anonymous because each intermediate node or onion router knows only the address or location of its preceding and following nodes.

Keywords: *Integrated Collective Node, Secured Data Transmission, Onion Protocol.*

1. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network. In Onion routing technique the sender and receiver remain anonymous. Messages sent through Onion network are encapsulated in several layers of encryption similar to that of the layers present in an onion. The data is transmitted through a series of nodes over the network and these nodes are called 'Onion routers'. Each onion router peels away a single layer and uncovers the data's next destination. And when the final layer gets decrypted in this process then the message arrives the destination. The sender remains unknown and anonymous because each intermediate node or onion router knows only the address or location of its preceding and following nodes.

In the EXISTING SYSTEM, there is no need for the key generating terminals to obtain correlated observations in channel. In the PROPOSED SYSTEM, we build a secret agreement protocol between the Nodes. For Example Bob & Alice can communicate with Each other with Relay as the Intermediate Medium. Bob & Alice Share their Primary & Secondary Keys to the Relay. Both the Keys are added together and made X-AND by server and Transmits the Corresponding Keys to both of them. This Key is used for Communication.

Objective: To avoid data hacking and perform the secure data transmission by encrypting the original data. The data is transmitted with signature & signature is verified for the security of the data transmission

2. LITERATURE SURVEY

[1] Title: Performance and Security Analyses of Onion-Based Anonymous Routing for Delay Tolerant Networks

Abstract: Delay tolerant network (DTN) routing provides a communication primitive in intermittently disconnected networks, such as battlefield communications and human-contact networks. In these applications, the anonymity preserving mechanism, which hides the identities of communicating parties, plays an important role as a defense against cyber and physical attacks. While anonymous routing protocols for DTNs have been proposed in the past, to the best of our knowledge, there is no work that

emphasizes analysis of the performance of these protocols. In this paper, we first design an abstract of anonymous routing protocols for DTNs and augment the existing solution with multi-copy message forwarding. Then, we construct simplified mathematical models, which can be used to understand the fundamental performance and security guarantees of onion-based anonymous routing in DTNs. To be specific, the delivery rate, message forwarding cost, traceable rate, and path and node anonymity are defined and analyzed. The numerical and simulation results using randomly generated contact graphs and the real traces demonstrate that our models provide very close approximations to the performance of the anonymous DTN routing protocol.

[2] Title: Epidemic Routing for Partially-Connected Ad Hoc Networks

Abstract: Mobile ad hoc routing protocols allow nodes with wireless adaptors to communicate with one another without any pre-existing network infrastructure. Existing ad hoc routing protocols, while robust to rapidly changing network topology, assume the presence of a connected path from source to destination. Given power limitations, the advent of short-range wireless networks, and the wide physical conditions over which ad hoc networks must be deployed, in some scenarios it is likely that this assumption is invalid. In this work, we develop techniques to deliver messages in the case where there is never a connected path from source to destination or when a network partition exists at the time a message is originated. To this end, we introduce Epidemic Routing, where random pair-wise exchanges of messages among mobile hosts ensure eventual message delivery. The goals of Epidemic Routing are to: i) maximize message delivery rate, ii) minimize message latency, and iii) minimize the total resources consumed in message delivery. Through an implementation in the Monarch simulator, we show that Epidemic Routing achieves eventual delivery of 100% of messages with reasonable aggregate resource consumption in a number of interesting scenarios.

[3] Title: Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks

Abstract: Intermittently connected mobile networks are sparse wireless networks where most of the time there does not exist a complete path from the source to the destination. These networks fall into the general category of Delay Tolerant Networks. There are many real networks that follow this paradigm, for example, wildlife tracking sensor networks, military networks, inter-planetary networks, etc. In this context, conventional routing schemes would fail. To deal with such networks researchers have suggested to use flooding-based routing schemes. While flooding-based schemes have a high probability of delivery, they waste a lot of energy and suffer from severe contention, which can significantly degrade their performance. Furthermore, proposed efforts to significantly reduce the overhead of flooding-based schemes have often be plagued by large delays. With this in mind, we introduce a new routing scheme, called Spray and Wait that "sprays" a number of copies into the network, and then "waits" till one of these nodes meets the destination. Using theory and simulations we show that Spray and Wait outperforms all existing schemes with respect to both average message delivery delay and number of transmissions per message delivered; its overall performance is close to the optimal scheme. Furthermore, it is highly scalable retaining good performance under a large range of scenarios, unlike other schemes. Finally, it is simple to implement and to optimize in order to achieve given performance goals in
Practice.

[4] Title: An Optimal Probabilistic Forwarding Protocol in Delay Tolerant Networks

Abstract: Due to uncertainty in nodal mobility, DTN routing usually employs multi-copy forwarding schemes. To avoid the cost associated with °ooding, much e®ort has been focused on probabilistic forwarding, which aims to reduce the cost of forwarding while retaining a high performance rate by forwarding messages only to nodes that have high delivery probabilities. This paper aims to provide an optimal forwarding protocol which maximizes the expected delivery rate while satisfying a certain constant on the number of forwardings per message. In our proposed optimal probabilistic forwarding (OPF) protocol, we use an optimal probabilistic forwarding metric derived by modeling each forwarding as an optimal stopping rule problem. We also present several extensions to allow OPF to use only partial routing information and work with other probabilistic forwarding schemes such as ticket-based forwarding. We implement OPF and several other protocols and perform trace-driven simulations. Simulation results show that the delivery rate of OPF is only 5% lower than epidemic, and 20% greater than the state-of-the-art delegation forwarding while generating 5% more copies and 5% longer delay.

[5] Title: Forwarding Redundancy in Opportunistic Mobile Networks: Investigation, Elimination and Exploitation

Abstract: Opportunistic mobile networks consist of mobile devices which are intermittently connected via short-range radios. Forwarding in such networks relies on selecting relays to carry and deliver data to destinations upon opportunistic contacts. Due to the intermittent network connectivity, relays in current forwarding schemes are selected separately in a distributed manner. The contact capabilities of relays hence may overlap when they contact the same nodes and cause forwarding redundancy. This redundancy reduces the efficiency of resource utilization in the network, and may impair the forwarding performance if being unconsciously ignored. In this paper, based on investigation results on the characteristics of forwarding redundancy in realistic mobile networks, we propose methods to eliminate unnecessary forwarding redundancy and ensure efficient utilization of network resources. We first develop techniques to eliminate forwarding redundancy with global network information, and then improve these techniques to be operable in a fully distributed manner with limited network information. We furthermore propose adaptive forwarding strategy to intentionally control the amount of forwarding redundancy and satisfy the required forwarding performance with minimum cost. Extensive tracedriven evaluations show that our schemes effectively enhance forwarding performance with much lower cost.

[6] Title: Efficient and Privacy-Aware Data Aggregation in Mobile Sensing

Abstract: The proliferation and ever-increasing capabilities of mobile devices such as smart phones give rise to a variety of mobile sensing applications. This paper studies how an untrusted aggregator in mobile sensing can periodically obtain desired statistics over the data contributed by multiple mobile users, without compromising the privacy of each user. Although there are some existing works in this area, they either require bidirectional communications between the aggregator and mobile users in every aggregation period, or have high-computation overhead and cannot support large plaintext spaces. Also, they do not consider the Min aggregate,

which is quite useful in mobile sensing. To address these problems, we propose an efficient protocol to obtain the Sum aggregate, which employs an additive homomorphic encryption and a novel key management technique to support large plaintext space. We also extend the sum aggregation protocol to obtain the Min aggregate of time-series data. To deal with dynamic joins and leaves of mobile users, we propose a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave. Evaluations show that our protocols are orders of magnitude faster than existing solutions, and it has much lower communication overhead.

[7] Title: Routing in a Delay Tolerant Network

Abstract: We formulate the delay-tolerant networking routing problem, where messages are to be moved end-to-end across a connectivity graph that is time-varying but whose dynamics may be known in advance. The problem has the added constraints of finite buffers at each node and the general property that no contemporaneous end-to-end path may ever exist. This situation limits the applicability of traditional routing approaches that tend to treat outages as failures and seek to find an existing end-to-end path. We propose a framework for evaluating routing algorithms in such environments. We then develop several algorithms and use simulations to compare their performance with respect to the amount of knowledge they require about network topology. We find that, as expected, the algorithms using the least knowledge tend to perform poorly. We also find that with limited additional knowledge, far less than complete global knowledge, efficient algorithms can be constructed for routing in such environments. To the best of our knowledge this is the first such investigation of routing issues in DTNs.

3. METHODOLOGY

EXISTING SYSTEM:

In the EXISTING SYSTEM, there is no need for the key generating terminals to obtain correlated observations in channel. In this system less data security is present and the transmission rate is low. There is loss of data and the eve node will affect the transmission path in this system.

PROPOSED SYSTEM:

In the PROPOSED SYSTEM, we build a secret agreement protocol between the Nodes. For Example Bob & Alice can communicate with Each other with Relay as the Intermediate Medium. Bob & Alice Share their Primary & Secondary Keys to the Relay. Both the Keys are added together and made X-AND by server and Transmits the Corresponding Keys to both of them. This Key is used for Communication. Over here high data security and high data transmission rate is present. The eve node is detected and removed. It has strong and secured transmission path and the data which gets missed will be recovered easily in this system.

MODIFICATIONS DONE:

In the MODIFICATION, Alice selects the routes for data transmission to Bob based on checking neighbor node capacity. After key assignment and route selection, Alice gives data with first half key to relay. If the keys are match means, relay sends the encrypted data to Alice based on RC4. Alice splits the data to three parts and sends the encrypted data to Bob through neighbor nodes on multiple routes. Bob sends the encrypted data with second half key to server.Then server check second half key of bob if both keys are match means, server sends the decrypted data to Bob. Suppose Eve node receives and forwards the encrypted data to server for view the original data means, server checks the keys if both are mismatch means, it easily identify the Eve node. Server also reconstructs the data based on erasure code technique.

MODULES:

Network Connection:

In the Project, server monitoring which consists of ‘n’ number of nodes. Then each node to connect the nearest node to established their connection and it also monitoring those bridge connections between nodes and server. The server are monitoring for all the nodes and are sharing their information like node id, primary key and secondary key with each other mobile nodes. Source requests are sent into neighboring nodes based on covered area within limitation of distance range. Then server covers and monitors the nodes under the certain region in the network.

Secure Packet Transmission:

Each node having node id and other security credentials for sharing their packet to destination from the source node. Server assigns primary and secondary keys for each node and do key pairing that is called mutual key. Key pairing is a process to generate a code by combining both keys and then split it into two encryption data from the source to destination and server. One of the parts is assigned for the Alice (source) and another for the Bob by the server. Key pairing is done by the Relay node till reach destination based on mutual key considered.

4. CONCLUSION

Hence in this system the data transmission takes place in a secured manner and the data transmission rate is very high after the modifications are done.

5. REFERENCE

[1] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, The, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] U. M. Maurer, “Secret key agreement by public discussion from common information,” Information Theory, IEEE Transactions on, vol. 39, no. 3, pp. 733–742, 1993.
[3] B. Kanukurthi and L. Reyzin, “Key agreement from close secrets over unsecured channels,” in Advances in Cryptology-EUROCRYPT 2009. Springer, 2009, pp. 206–223.

[4] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," Information Theory, IEEE Transactions on, vol. 54, no. 6, pp. 2437–2452, 2008.
[5] E. Ekrem and S. Ulukus, "Secrecy Capacity of a Class of Broadcast Channels with an Eavesdropper," EURASIP J. Wireless Comm. And Networking, 2009.
[6] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," NetCod, Apr, vol. 104, 2005
[7] Y. Wei, Z. Yu, and Y. Guan, "Efficient weakly-secure network coding schemes against wiretapping attacks," in Network Coding (NetCod), 2010 IEEE International Symposium on. IEEE, 2010, pp. 1–6.

