International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Fast and Secure Packet Scheduling with Packet Level Redundancy Elimination in Dynamic Mobile Networks

K.Soniya, A.Senthil Kumar

Abstract: ***Mobile networks are fast and flexible for effective communication, where it only needs a dynamic topology and unstructured network construction. Due to this flexible nature, the resource utilization and energy consumption is high when comparing to the other static networks. In this scenario, packet redundancy is major problem on mobile networks, which increases network traffic and energy. Currently redundancy elimination is performed using redundancy elimination (RE) solution, which affects the end-to-end privacy. To eliminate redundant packet transfers and provide fast and secure packet transfer in the dynamic mobile network, a new middle box framework is proposed in this paper. This framework is named as Sift Hub, which is a centre point to verify the packet redundancy and security violations. This includes four algorithms to perform packet redundancy elimination, packet scheduling and verification. The algorithms are One pass signature generation algorithm (OSGA) for packet security, Predictive encryption technique using enhanced hidden vector encryption algorithm for redundancy detection on encrypted traffic, Packet level data filtering algorithm (PLDF) for eliminating un-authenticated and redundant packets and RAPS-Redundancy aware packet scheduling algorithm for fast data scheduling over dynamic mobile networks. The Shift_Hub supports inter and intra packet level redundancy elimination and secure packet scheduling without affecting the end-to-end privacy. The Shift_Hub is implemented and the performance is evaluated on dynamic mobile network scenario created on NS2 simulator. The results shows, the proposed work gives better performance in finding and eliminating redundant packet in secure manner than the existing works.***

Keywords: Mobile Networks, Middle box, Packet Scheduling, Redundancy elimination.

I. INTRODUCTION

Mobile Networks (MN) comprising of a vast range of mobile nodes are generally employed in totally different applications. Each mobile node contains many elements and works severally. Dynamic mobile networks are developed for transferring knowledge among totally different users and provide numerous personal info sharing, social knowledge gathering, health and academic connected file sharing etc.

Manuscript published on November 30, 2019.
* Correspondence Author
K.Soniya*, Research Scholar, Department of Computer Science, Sankara College of Science and Commerce, Coimbatore, India. Email: sony.krishnaraj53@gmail.com
Dr.A.Senthil Kumar, Associate Professor, Department of Computer Science, Sankara College of Science and Commerce, Coimbatore, India. Email: senthask@gmail.com

like this several applications are embedded with the mobile networks . Most of those applications have interaction a distributed system of mobile users. The setting is transferring scores of knowledge from one to a different. Therefore, knowledge transferring on timely manner will be viewed as a necessary building block in mobile networks.At the time of information transfer of victimization mobile networks, a couple of stuffs are highly regarded, and this definitely leads to an outsized quantity of network traffic over mobile networks being redundant since multiple users at a similar server might request same or similar content.
Therefore, the mobile links carry identical contents additionally to identical requests on a daily basis. To eliminate these redundant traffic problems while not violating privacy and avoid congestion, several systems are projected and deployed. This leads to less information measure consumption, restricted energy consumption and reduced delay. To perform this, cache ideas are enclosed. This cache method fetches the information content from the server and distribute to the n range of mobile users once the request is formed on same content. This considerably improves the reaction time within the information service. However, this can be extremely appropriate for the similar content request created by the users. But, the matter is, once the user sends a dynamic content with packet redundancy, the cache ideas are unsuccessful.

To address this downside, a brand new framework "sift-hub" is intended and enforced, the planned system eliminates redundancy of network traffic at packet-level and furthermore as user-level directly over encrypted traffic while not decryption it. And this conjointly provides high security and privacy protective for information contents at the time of verification, finally packet programming is performed supported the redundancy issue. During this manner, Sift-Hub keeps the network economical while not compromising the security/privacy of user information.
The remaining of the paper is planned as follows. In the following, we tend to shortly describe the packet-level redundancy elimination and packet programming techniques, and discuss the planned work. In Section three, we tend to discuss the four algorithms and also the framework intimately. Section four provides the implementation and results of the planned work, and eventually section five concludes the work.

II. LITERATURE REVIEW

Content redundancy elimination is a vital to create the network performance more practical. Numerous Redundancy Elimination systems are deployed.

For such object-level redundancy elimination (RE) systems, a lot of work has been done [1],[2]. However, the loss of power to eliminate duplication between packets to totally different consumer protocols and solely operates if finish users request similar content that has antecedently appeared. The opposite approach [3] operates on the premise of the packet. It leverages network middle boxes to delete all computer memory unit strings that regularly seem across packet payloads, regardless of the appliance layer protocols used. This technique is usually applied to the IP or transmission control protocol layer to cut back computer memory unit coarseness consistency and thus has finer granularity. Whereas comparison with the objective-level technique from the literature, this approach is more practical for the aim of RE [4], [5].

The packet-level RE is therefore turning into additional common and widespread industrial implementations are seen [6], [7]. The WAN improvement market is predicted to rise to over $12B by 2019[8]. Nonetheless, current packet-level RE ways aren't any longer operating with the growing acceptance of HTTPS and alternative authentication protocols. This can be as a result of middle boxes cannot examine payload, plus eliminate redundancy in traffic, once packet payloads are encrypted by TLS / SSL. In fact, businesses either ought to shut off SSL or hand over RE's advantages.

Some presently deployed Redundancy Elimination systems, claiming to support HTTPS, really grant access to session keys to service suppliers so as to rewrite traffic in middle boxes[7],[9]. This strategy undermines SSL's end-to-end security guarantee and might not defend the privacy of users from service suppliers putting in the middle boxes. In reality, service suppliers used their deployed middle box to capture net traffic for observation and advertising functions [10],[11] a apply that has received tons of criticism.

Spring and Wetherill [3] introduced the protocol freelance packet-level RE for the primary time and saw giant business implementation as a part of Wide Area Network optimization. Strategies for packet-level RE are typically available based on middle box and end-based. There has been tons of follow-up add this area [5],[13],[15]. Such associate degree approach needs RE middle boxes to be put in on access routers wherever packets enter or leave a stub network. Thus, inter- and intra-user RE will be supported. A long-standing middle box-based answer issue, however, is that middle boxes don't handle encrypted traffic well. Whereas some middle box-based solutions claim to support SSL, they lack end-to-end security guarantees [7],[9].

On the opposite hand, end-based RE system [4] will offer benefits for protocols like HTTPS as payload is compressed before encoding. Such a pure end-to-end approach, however, solely advantages intra user RE and will lose potential savings of twenty five p.c from inter-user redundancy.

Additionally, since the memory capability on associate degree finish system is restricted, redundancy intra-user can't be eliminated fully. During this paper, while not compromising the benefits of middle box or end-to-end encoding, middle box-based RE answer has recently been planned by authors that allows each to exist.

III. PROPOSED WORK

3.1 Contributions:

The proposed system develops and implements an efficient framework "Sift-Hub" for solving the packet redundancy and scheduling issues in dynamic mobile networks on encrypted traffic. The work extends the existing **RE over encrypted traffic (REET)** [12] approach in the network with effective packet scheduling and privacy preserving. In the packet scheduling different delays are calculated and this delay calculation helps to know the traffic of the link. This computes the queue delay, propagation and transmission delay. Implementation of the Sift-Hub" in mobile network assists reducing the complexity of calculating packet-level and user level redundancy of every mobile node over a period of time. The framework concept effectively uses the dynamic work load calculation and packet scheduling without redundant content. Finally, the proposed system works with the following algorithms and techniques.

1. One pass Signature Generation Algorithm (OSGA)for generating unique signature for every user and packet.
2. Predictive encryption technique using enhanced hidden vector encryption algorithm is designed to perform the detection of redundant content over encrypted data without affecting privacy.
3. Packet level data filtering algorithm (PLDF) developed to eliminate/re-schedule the redundant and un-secure data packets.
4. Finally, a scheduling algorithm is developed and named as "RAPS"(Redundancy aware packet scheduling algorithm) for cost effective and traffic free path selection.

The proposed distributed enhanced packet filtering and scheduling approaches reduce service disruption and minimize the packet redundancy in both packet-level and user level. Every packet will be analyzed and updated in the Sift-Hub using different algorithms. The proposed framework adopts four algorithms in mobile networks. The proposed work is results in congestion avoidance and provides high performance in terms of congestion, overhead, transmission delay, queuing delay, propagation delay, mobility-resilience, traffic reduction and scalability. The overall architecture implemented framework is as follows.

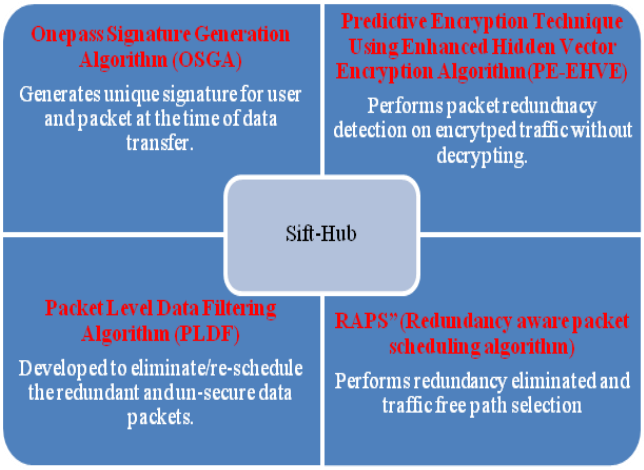

Figure-1. Architecture Sift-Hub framework for mobile networks

Fig 1 shows the set of processes included in the Sift-Hub architecture. The name of the framework indicates the examination center, which is defined a middle box that works on different layers of network rather than the application layer. The OSGA, PE-EHVE, PLDF and RAPS are explained below in detail.

3.2 Sift-Hub:

The proposed framework for mobile network involves different process such as node initiation with one pass signature generation process, later the packets are encrypted and transmitted using PE-EHVE and it also finds the redundancy on encrypted content without decrypting them. The improvement on the existing hidden vector encryption and REET is made to create the new algorithm. After finding packet-level redundancy, the packets will be eliminated using PLDF algorithm. This keeps a buffer for the eliminated content for a particular time and eliminates permanently if the time limit exceeds. Finally, the rest of the contents which are unique is transferred via a traffic free and cost effective path in the network. The proposed work involved with various layers for providing security, privacy, redundant and traffic free data routing.

3.2.1: Connection setup and OSGA:

The initial process in the network scenario is setting up the connection for the simulation and generating Onepass signature for the mobile users. This eliminates the creation of key from random key generation, and generates an unique signature using OSGA algorithm. Here, the given user information D is divided into chunk and computes the O=Op(D, α) . Where, Op is the pre defined Onepass signature function and the D is the data, and O is the Onepass signature key for further process.

OSGA Steps:

Step 1: Initiate
Step 2: Get user info as plain vector D,
Step 3: D, O ← Setup (∀)
Step 4: O_T ← O_c (∀) Set key for time
Step 5: Os ← O, generated signatures are stored in Os.
Step 6: End

From the above algorithm, the connection setup is performed and Onepass signature is generated for all nodes in the communication process. The user information's such as node id, location, name, time of initialization is stored in D. and based on that, the O is generated. Here O is the Onepass signature key. O_T denotes the key for the time interval which is similar to the session. O_c refers the input string which contains sequence set of key for signature key generation. The generated Onepass signature is stored in O_S and distributed to the mobile users.

3.2.2 Signature Distribution:

The next process of the Sift-Hub is transmitting the generated signature to the protocol based on demand. This is done using a basic routing process with tiny packet to the authorized mobile user form the Sift-Hub point. The packet transmission is performed using application layer to the transport layer using TCP (Transmission Control Protocol). Send $\boldsymbol{S_P \rightarrow (\forall M_N , IP)}$, where, $\boldsymbol{S_P}$ is the signature packet distribution procedure, this sends the signature for all mobile node ($\boldsymbol{M_N}$). it uses the mobile node IP address. The main objective of this process is achieving secret sharing of signatures to the mobile nodes. So the next process encrypts the data and transmits to the user.

3.2.3 Predictive encryption technique using enhanced hidden vector encryption algorithm:

In Sift-Hub, contents are encrypted victimization PE-EHVE rule, which may perform quick content verification over encrypted content. The coding method ab initio performed at the sender facet with tokenizing. The coding method is denoted in step a.

a. The PE-EHVE rule takes as input a vector x = (x1,...,xl) ∈ Σ l , a knowledge D ∈ D and therefore the one pass signature key O. It outputs a cipher text CT for x and D.

The prophetical coding theme performs verification of content over encrypted content while not decrypting, for this, it performs the subsequent perform b.

b. Verify (CT,TKσ,O). The search rule takes as input a cipher text CT, a token TKσ for a vector σ that corresponds to a predicate fσ, and therefore the one pass key O. It outputs M if fσ(x) = one or outputs ⊥ otherwise.

The coding and verification method are done by PE-EHVE rule for each information D victimization the vector as input and therefore the one pass signature from the OSGA part. The planned work eliminates the information measure overhead, wherever it's vast in existing thanks to excess coding of all tokens within the traffic. this will be illustrated employing a packet S is taken into account as N bytes that assumes SN≥T, wherever T is that the total bytes for tokenization. the worth of T is among sixty four bytes, this lead to high information measure overhead by process SN-T+1 token. However the planned rule is light-weight and occupies less memory by choosing giant interval tokens for coding method.

3.2.4 Packet Level Data Filtering Algorithm (PLDF):

In mobile network, content privacy, packet security, filtering redundant and unsecure data are the most important needs particularly when the mobile network is highly dynamic and resource constrained. After successful verification and file transmission initialization process, identified redundant packets are filtered using PLDF algorithm. This keeps a buffer about the eliminated content. In such a situation, packet filtering method helps to manage up with these issues. Packet filtering without decryption using PE-EHVE will decrease the number of data packets broadcasted and the data variance, thus increase the data correctness and data transfer efficiency through the redundant data in the network.

3.2.5 Redundancy Aware Packet Scheduling algorithm (RAPS):

This formula Performs packet programming supported the redundancy elimination output. This calculates the priority of information packets by its content quality and selects best link supported numerous factors. the essential construct of RAPS is that each node constructs a map of the property to the network, showing that nodes are connected to which alternative nodes. every node then severally calculates subsequent best logical path from it to each attainable destination within the network. The projected section gathers link state data from accessible routers and constructs a topology map of the network. The topology determines the routing table that makes routing selections. it detects changes within the topology, like link failures, terribly quickly and converges on a brand new QOS secure routing structure inside seconds.

It computes the weighted path structure for every route employing a methodology primarily based RAPS.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section described the Simulation parameters, simulation tool, and simulation results. The performances of the proposed Sift-Hub framework with the set of algorithms are compared with the existing technique are evaluated on the basis of the performance matrices.

4.1 Simulation Parameters:

NS2 machine is employed to simulate the planned system. Within the simulation, the data rate and alternative resources are such and valid from that.

within the simulation, total range of mobile nodes are fifty those nodes are haphazardly deployed in an exceedingly one thousand x 1000 m region for 250 seconds simulation time. All nodes have identical transmission vary of 250 meters. The simulated traffic is Constant Bit Rate (CBR). The simulation settings are summarized within the Table one.

Table I Simulation parameters

Parameters	Value
Number of Nodes	Fifty(50)
Area Size	One Thousand X 1000
Simulation Time	Two Hundred Seconds
Traffic Source	cosmic microwave background radiation
Packet Size	512
Transmit Power	0.360 w
Receiving Power	0.395 w
Idle Power	0.335 w
Initial Energy	5.0 J
No. of sources	4
Transmission Rate	250,500,750 and 1000 kb.

4.2 Results

A simulation study was disbursed to judge the performance of the secure version of mobile network routing techniques REET-AODV, and AODV supported the metrics outturn, packet delivery magnitude relation and average time quality with the subsequent parameters: at the start this sections describes concerning the performance of the SIFT-HUB in numerous factors and at last this performs the comparative study with the prevailing algorithms and protocols. the subsequent table two shows the extra simulation parameters for the implementation. This specifies the radio model, packet size used for transmission alongside the fundamental protocol.

Table II Simulation parameters employed for the comparative study

Parameter	Value
Radio model	TwoRay Ground
Protocols	AODV
Packet size	512 bytes

So the simulation has increased from the AODV protocol. SIFT-HUB has used many ideas of AODV for effective packet filtering and packet programming. The planned system works with efficiency and produces optimum resolution albeit the network contains terribly sizable amount of mobile nodes and packets. The signature creation time and sharing among mobile nodes are attenuate. The performance is compared with many parameters to prove the effectiveness of the planned system supported the amount of tokens within the packet.ie supported packet count that are initiated to transmit over the network.

4.2.1 Time Complexity

The time quality of the projected rule is O (n), as a result of the performance can grow linearly and in direct proportion to the entire range of computer file assortment. The time taken for various methods is given within the table three.

Table III Time complexity analysis table

File size (MB)	*Encryption time*	Verification time
512	*23*	12
1024	*41*	18
2048	*69*	26

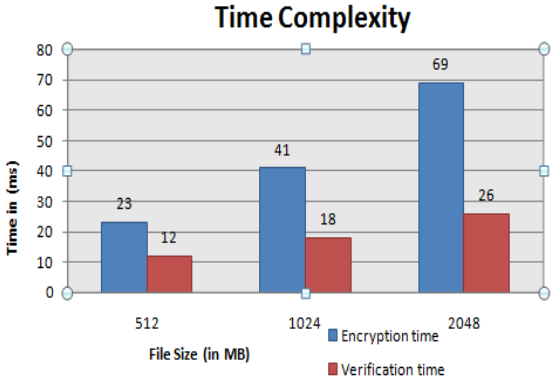

Figure-2 Time analysis for different process in the proposed system

The Figure 2 shows the time consumption for encryption, and verification time on encrypted traffic for finding redundant traffic This shows, the verification time is reduced due to the effective byte verification system using PE_EHVE algorithm

4.2.2 Throughput

It is the quantitative relation of the most quantity of information from a recipient to the time it takes for the receiver to urge the last packet. When scrutiny the routing outturn by each of the technique,

Shift-Hub has high outturn. As a result of the use of packet programming decreases the congestion and redundant packet elimination will increase the information measure utilization. It measures of effectiveness of the projected work.

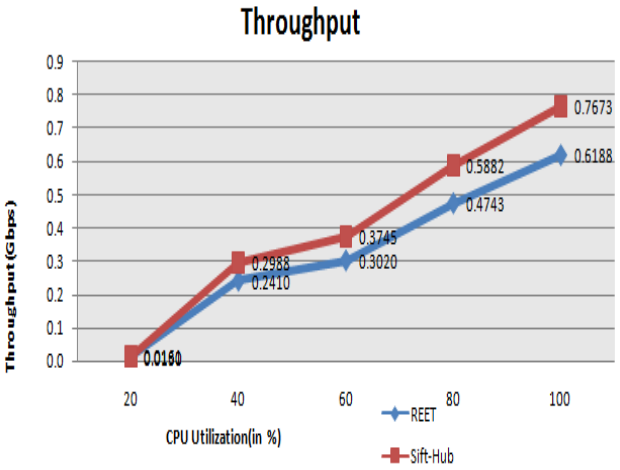

Figure 3 Throughput comparison chart

First we have a tendency to compare the sender aspect against use of the central processing unit as shown in Fig. 3. Such numbers embrace the time to get Onepass, the multi-layer authentication and also the method of transmission. Every box shows the vary of the performance given the employment of the central processing unit, this has been compared with the present REET and also the output is higher within the projected Sift-Hub.

V. CONCLUSION

Elimination of redundant packet and un-authenticated packet within the mobile network can greatly impact on the resources saving. So, the projected work developed a replacement framework named as "Sift-Hub" for mobile network to effectively cut back the redundant packets and permitting them in a very well fashioned network routing method. The projected work consists of 4 algorithms for various methods. And multi-layer design is employed for the implementation. The projected work is ready to support on each lay to rest and intra user and packet level redundancy elimination on encrypted traffic. This extremely preserves user privacy at the time of verification. The projected work is compatible with the normal technique in RE and REET over unencrypted traffic thus permits the employment of multi layer framework to perform packet-level and user level RE. The performance analysis demonstrates that Sift-Hub provides high security and privacy-preserving RE with high outturn and restricted time complexness for cryptography and verification when put next to the REET solutions.

REFERENCES

1. L. Fan, P. Cao, J. Almeida, and A. Z. Broder, "Summary cache: A scalable wide-area Web cache sharing protocol," *IEEE/ACM Transaction Network.*, Volume. 8, Number. 3, pp. 281–293, 2000.
2. Wolman , M. Voelker, N. Sharma, N. Cardwell, A. Karlin, and H. M. Levy ., "On the scale and performance of cooperative Web proxy caching," *ACM SIGOPS Operating. System. Rev.*, Volume. 33, Number. 5, pp. 16–31, 1999.
3. N. T. Spring and D. Wetherall, "A protocol-independent technique for eliminating redundant network traffic," *ACM SIGCOMM Computer.Commun. Rev.*, Volume. 30, Number. 4, pp. 87–95, 2000.
4. B. Agarwal, A.Akella,D.Anand., "Endre: An end-system redundancy elimination service for enterprises," in *Proceedings. NSDI*, 2010, pp. 419–432.
5. Anand, A. Gupta, A. Akella, S. Seshan, and S. Shenker, "Packet caches on routers: the implications of universal redundant traffic elimination," *ACM SIGCOMM Comput. Commun. Rev.*, Volume. 38, Number. 4, pp. 219–230, 2008.
6. Dr.A.Sentil kumar, "A Survey on Agriculture Analysis for Crop Yield Prediction Using Data Mining Techniques'" , *IOSR*, Volume. 1, 2018.
7. *WAN Optimization*. Accessed: October 2019 . [Online]. Available: https://www.silver-peak.com/solutions/wan-optimization
8. *WAN Optimization-WAN Technologies From Riverbed*. Accessed: October 2019. [Online]. Available: http://www.riverbed.com/solutions/wanoptimization. html
9. *WAN Optimization Market Worth $12.1 Billion by 2019*. Accessed: October 2019. [Online]. Available: http://www.marketsandmarkets.com/PressReleases/wan-optimization.asp
10. *Cisco Wide Area Application Services SSL Acceleration Technical Overview*. Accessed: October 2019. [Online]. Available:http://www.cisco.com/c/en/us/products/collateral/routers/wide-areaapplication-services-waas-software/solution_overview_c22-532534.html
11. *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*. Accessed October 2019. [Online]. Available: https://www.propublica.org/article/nsaspying- relies-on-atts-extreme-willingness-to-help
12. *AT&T is Going to Start Selling Your Dat, So Here's How You Can Opt Out*. Accessed: October 2019. [Online]. Available: http://www.huffingtonpost.com/2013/07/08/att-selling-data_n_3561263.html
13. Fan, J., Guan, C., Ren, K., & Qiao, C. (2018). Middlebox-based packet-level redundancy elimination over encrypted network traffic. IEEE/ACM Transactions on Networking (TON), 26(4), 1742-1753.
14. A. Anand, C. Muthukrishnan, A. Akella, and R. Ramjee, "Redundancy in network traffic: Findings and implications," *ACM SIGMETRICS Perform. Eval. Rev.*, Volume. 37, Number 1, pp. 37–48, 2009.
15. A. Shamir, "How to share a secret," *Commun. ACM*, Volume. 22, Number. 11, pp. 612–613, 1979.
16. A. Anand, V. Sekar, and A. Akella, "Smartre: an architecture for coordinated network-wide redundancy elimination," *ACM SIGCOMM Comput. Commun. Rev.*, Volume. 39, Number. 4, pp. 87–98, 2009.

AUTHORS PROFILE

M.Phil Research Scholar, Department of Computer Science, Sankara College of Science and Commerce, sony.krishnaraj53@gmail.com.

Associate Professor, Department of Computer Science, Sankara College of Science and Commerce, senthask@gmail.com.