International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
National Conference on Advances in Engineering and Technology
(AET- 29th March 2014)

RESEARCH ARTICLE OPEN ACCESS

Secured Caching Strategy for Information Sharing in VANETs

Savita Korram*, Naveen Chauhan**
*(Department of Computer Science and Engineering, NIT Hamirpur, India
Email: savita_nith@yahoo.in)
** (Department of Computer Science and Engineering, NIT Hamirpur, India
Email: naveenchauhan.nith@gmail.com)

ABSTRACT
With high mobility, it is barely easy for the vehicles to access confined data in VANETS and to overcome this difficulty data is being stored in local storage of vehicles. Although a lot of research work has been done on efficient information sharing, security issues are largely ignored in these works. Therefore, our work is mainly focused on securing valuable information that is shared among the nodes. A key design optimization technique of this paper is to prevent the legitimate nodes from malicious nodes which may return the cached data or modify the route and forward a request to a caching node. This paper includes an authentication mechanism, preventing mobile nodes from maliciously modify data, drop or forward the request to the wrong destination. This efficient caching technique in cooperative fashion to allow the sharing and coordination of cached data among multiple nodes, can be used to improve the performance of data access in VANETS. In addition to the above technique, a cache invalidation scheme is also addressesd to keep the cached copies valid.

I. INTRODUCTION

VANET is one of the new types of Mobile Ad-hoc Networks and the most promising networking paradigm that received strong interest from research communities. Network with high-speed mobile vehicles providing information to vehicular passengers is one of the most promising directions of the mobile infotainment business. Unfortunately, information delivery to moving vehicles is also a most challenging task. Cooperative Caching is an effective technique to cache the frequently accessed data items at the client side to improve performance in mobile environments [9][10]. To reduce data access delay, caching technique is being used since some data access requests can be served from the local cache, thereby obviating the need for data transmission over the scarce wireless links. As mobile nodes in ad hoc networks may have similar tasks and share common interests, cooperative caching [1], which allows the sharing and coordination of cached data among multiple nodes, can be used to reduce the bandwidth and power consumption. For example, if a vehicle obtained the accidental information from the data centre, it is very likely that nearby vehicles also need the same information from the data centre. Bandwidth and power can be saved if these data accesses are served by the vehicle with the cached data instead of the data centre, which may be far away. Certainly, this cache sharing requires mobile nodes to coordinate with each other regarding their cached data then it can communicate with other cars and can warn those cars which are not yet arrived at accidental place thus using Vehicle-to-Vehicle (V2V) communication. This information may also be sent to or from roadside base units using Vehicle-to-Infrastructure (V2I) communication.

When cache is used, cache consistency issues [4] must be addressed to ensure that clients see only valid states of the data or at least do not unknowingly access data that is stale according to the rules of the consistency model [11][12]. In some adversary and strategic scenarios such as in the battlefield, accessing stale data (e.g., outdated enemy information) may be life threatening, and hence we need to study how to achieve strong consistency.

Considering later issue in caching, it is imperative to consider security as one of the issue which also affects the performance of the network. Since, the cached data may be returned by the mobile nodes, or modify the route and forward a request to a caching node, it is very important that mobile nodes do not maliciously modify data, drop or forward the

request to the wrong destination. In few researches some methods have been proposed to avoid or detect such malicious nodes via authentication mechanisms. Digital signature is one of the common approaches for data authentication. With this approach, the data source can sign the data with its private key, so that intermediate routers cannot modify the data. However, the digital signature approach has high overhead, both in terms of time to sign ands verify, and in terms of bandwidth.

A scheme for provisioning security in Data Caching to achieve more deterministic network behaviour, so that information carried by the network can be better delivered and network resources are better utilized. Following work is contributed:

(a) Efficient Cooperative Caching technique used to improve the performance of data accessibility.

(b) To protect the data accessibility from malicious nodes and also to improve the performance of network by providing better QoS from security.

(c) A cache invalidation scheme to invalidate the cached copies when the original data items are updated.

After accepting a service request from users, network has to ensure certain service requirements such as minimum bandwidth, maximum delay variance (jitter), maximum delay, and maximum packet loss rate etc. Thus, the network services can be characterized by all these set of measurable pre specified service which helps to meet users flow. In this research, we design and evaluate techniques to reduce such overhead and balance system performance and security strength. The final utility of the caching technique should be to impose fewer overheads on the network and take fewer resources, while at the same time making sure that more data is available with quality of information to the users.

The rest of paper is organized as follows. The prior work is analysed and the proposed schemes are presented in Sections II and III, respectively. Section IV is devoted to performance evaluation and comparison. Finally, the paper is concluded with future directions in Section V.

II. ISSUES CONCERNING DATA CACHING IN VANET

There are several challenging issues to improve the efficiency of data access in wireless ad hoc networks [13]. First, scarcity of communication bandwidth and resources: For example, sensor networks can only have at most a gross data rate with 250kbps in the physical layer. Second, increase the traffic load of net-works due to the transmission of large number of datum. In wireless mesh networks, streaming services are becoming much more popular, and some real-time applications require quality of services (QoS) guarantees, such as real-time surveillance [14]. Third, if users are mobile, they form a mobile ad hoc network such that dynamic topologies exacerbate the performance of the algorithms designed for static topologies. Fourth, Security of VANETs: one of the critical issues because their information transmission is propagated in open environments. Thus the system must be able to detect the obligation of drivers while still maintaining their privacy. To overcome the problems above, an effective caching system for VANET needs to provide a solution that takes all of these issues into consideration.

III. RELATED WORK

In the context of ad hoc networks, it is beneficial to cache frequently accessed data not only to reduce the average query latency but also to save wireless bandwidth. Similar with the case of Vehicular Ad hoc Networks, several proposals have been made to solve the issues related to data caching in adhoc networks.

In [1], a number of schemes related to caching have been proposed. First scheme, distributed caching strategies for ad hoc networks are presented according to which nodes may cache highly popular content that passes by or record the data path and use it to redirect future requests. To reduce the cache space requirement conservative rule, "*A node does not cache the data if all requests for the data are from the same node*" is designed. This scheme significantly reduces delay but does not guarantee quality of services such as security concerns, bandwidth utilisation etc. In [2], the solution that was proposed is based on the formation of an overlay network composed of mediator nodes, and it is only fitted to static connected networks with stable links among nodes. As it is not at all suitable for vehicular ad hoc networks but by exploiting mediator nodes from this papers and considering as relay nodes, will forwards the data to the other nodes. Thus this idea will help in providing efficient data accessibility. In [3], to improve data availability and access performance, COOP addresses two basic problems of cooperative caching i.e., cache resolution and cache management. One vehicular ad hoc network scenario is addressed in [4], where the authors proposed both an information retrieval technique that aims at finding the most popular and relevant data matching a user query and a popularity-aware data replacement scheme. In [5], decision of caching the data items depends on two factors, access affinity on the data items and mobility of each node. In [6], author proposed an algorithm for cache replacement problem on a network with

dynamic topology. Based on the above problem, author tried to detect the variation of contentions on a wireless node in order to select cache nodes for the optimal trade-off between the traffic cost and average query delay. In [7], author proposed a Group Caching approach to reduce the redundancy of cached data objects because the *MHs* can check the caching status of other group members for deciding the placement and replacement. Because more cache space can be utilized, each *MH* can store more different data objects in a group and then increases the data accessibility. A node that receives the requested information has the option to cache the received content and thus become a provider for that content to the other nodes. Determining a strategy of taking such caching decisions is the main objective of [8]. These researches are mostly based on improving query delay in data caching, which is also responsible in degradation of quality of services. But one thing must be kept in mind that without provisioning a secure transmission one cannot provide an efficient data caching scheme.

From previous research papers, provisioning secured data access for improving the efficiency of data caching scheme in VANETs has not yet taken into consideration. Therefore, implementing such strategy in the proposed data caching scheme is the main objective.

IV. SYSTEM MODEL

In this section, initially a simple vehicular ad hoc network model is described. Later, proposed model has been explained with the help of flow chart.

4.1 Network Model

Considering a simple VANET with cooperative communications, where each vehicle has the ability to relay data packets to each other. Assumption in this study are two-hop relays, comprising of a source (S), destination (D), and K relay nodes, R_1, R_2,...., R_k,....., R_k, as shown in Fig 1. The source node can send information to the destination directly or through a relay. In this approach, the router node caches those data which are frequently accessed. For example, if request d_i is forwarded through some relay nodes, R_1……R_k to the destination, D and the same request is demanded by other vehicle.

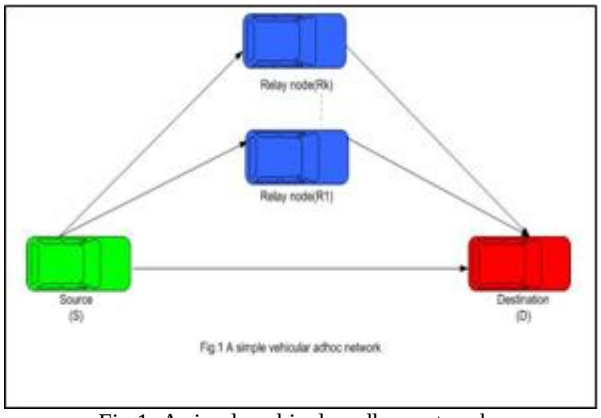

Fig 1: A simple vehicular adhoc network

4.2 Algorithm

The exact algorithm is followed by a node upon reception of a query message is detailed in the flowchart in Fig 2. Once information message is generated, it is being sent to the source after authentication process is completed. This process has been exploited from Adaptive and Lightweight Protocol for Hop-by-hop Authentication (ALPHA) signature scheme [15].

It would be of no use, if the data item provided to the clients are not the needed one. So here, in this paper our aim is not just to enrich the clients with the data items but also to facilitate with correct and updated data. For this purpose, the mobile clients have to make sure that the cached data is consistent with the data at the data centre. And to resolve cache consistency problem, strong cache consistency is taken into consideration. To prevent malicious nodes from modifying the invalidation messages, exploiting ideas from the IR-based cache invalidation [16]. In this approach, the server periodically broadcasts an invalidation report (IR) in which the changed data items are indicated. The IR consists of the current timestamp Tcur and a list of tuples (d_i; t_x) such that $t_x > (T_{cur} - w * L)$, where d_i is the data item id, tx is the most recent update timestamp of d_i, and w is the invalidation broadcast window size.

According to the proposed scheme, let us examine the detail operation of the secure cooperative cache scheme.

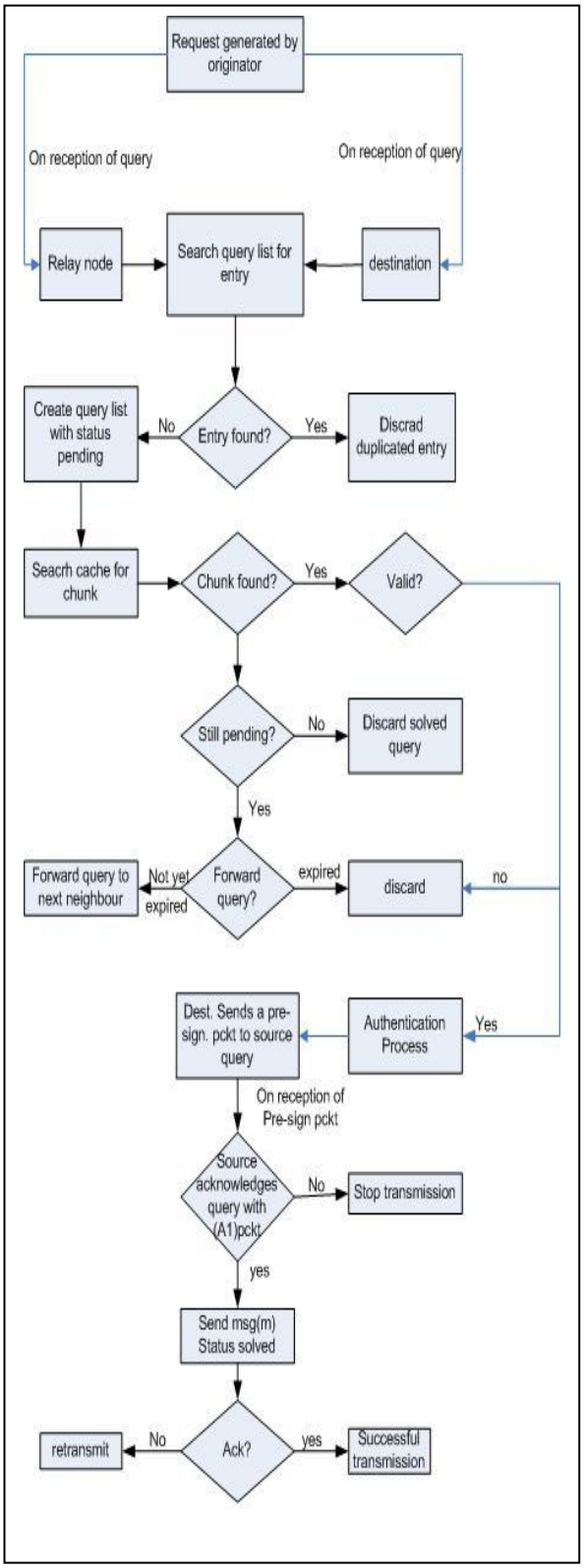

Fig 2: On reception of query

Considering a scenario of two vehicles (relay node/destination), one is the vehicle, v_y generates a query request for information c_i's chunks, d_{ic} which is not yet cached, v_y sends a request packet for accessing the data item to the another vehicle, v_x (chunk provider). Whenever the data item is updated the server generates an IR, $[id(d_i), vid(v_{ic,N}), T_{cur}]$, where T_{cur} is the current timestamp. Here are following steps:

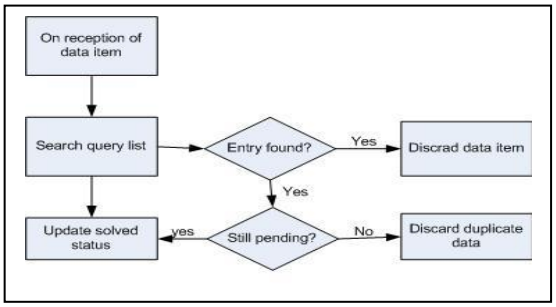

Fig 3: On reception of information

1. Query Request by vehicle, v_y: Query contains vehicle id (vid) and data item id, $[id(d_{ic})]$
   $= [id(d_{ic}), [vid(v_{ic,y})]]$,
   where $v_{ic,y} = \{v_y | request(d_{ic}), y \in N \wedge d_{ic} \in D\}$
   D = no. of data items
   N = no. of vehicles

Each signature packet exchange is initiated with an S_1 packet from the signer to the verifier. This packet fulfils three objectives. First, a fresh hash chain element of the signer's signature chain h_i^{Ss} identifies the signer. Second, a MAC keyed with the signer's next undisclosed signature chain element M (h^{Ss}_{i-1}; m) ensures the integrity of m. Therefore,

2. Reply forwarded to the query source (v_y) by the data item provider (v_x) : $[id(d_{ic}), [vid(v_{ic,x})], t_{ic,y}, S_1]]$, where $S_1 = [h_i^{Ss}, M(h_{i-1}^{Ss} | m)]$ and $t_{ic,y}$ = access time of d_{ic} by d_y

Third, the S_1 packet triggers the verifier to send an acknowledgment packet A_1.

3. For authenticating A_1 packet, the verifier (v_y) attaches the next undisclosed hash chain element of its acknowledgment chain h_i^{Va} to the A_1. Since, $A_1 = [h_i^{Va}, h_i^{Ss}]$.
4. On receipt of a valid A_1 packet, the signer discloses the key of the MAC h_{i-1}^{Ss} and the message m in the S_2 data packet. Where $S_2 = [h_{i-1}^{Ss} | m]$

With this key, the verifier and all relays that buffered $M(h_{i-1}^{Ss} | m)$ can check the integrity of m by recomputing the MAC. After the successful completion of authentication process, source acknowledges destination about reception of the message. On the reception of message finally the

whole transmission completes which is explained in Fig 3 with the help of flow chart and in case no acknowledgement is being received from source side then message is again generated by the destination.

V. CONCLUSION

This paper presents an algorithm which improves the performance of data access through secured cooperative caching technique for vehicular ad hoc networks whose nodes, exchange information items in a peer to peer fashion. A secured caching scheme which protects the legitimate nodes from being attacked by the malicious node as well as reducing the network overhead is presented. Also the cache or the available resources can be efficiently utilised. Conceivably, this paper can be extended in the future by addressing query delay problem and can explore more. This scheme is different and more efficient than previous caching scheme as security services is not yet provided in any caching strategy

REFERENCES

[1]. L. Yin and G. Cao, "Supporting cooperative caching in ad hoc networks" *IEEE Trans. Mobile Comput., 5(1), 2006, 77-89.*

[2]. N. Dimokas, D. Katsaros, and Y. Manolopoulos, Rongxing Lu, Chenxi Zhang, Haojin Zhu, "Cooperative caching in wireless multimedia sensor networks", *ACM Mobile Netw. Appl., 13(3/4), 2008, 337-356.*

[3]. Y. Zhang, J. Zhao, and G. Cao "Roadcast : A popularity-aware content sharing scheme in VANETs", *Proceeding of IEEE International Conference on Distributed Computing System, Los Alamitos, California, 2009, 223-230.*

[4]. Y. Du, S. K. S. Gupta, and G. Varsamopoulos "Improving on-demand data access efficiency in MANETs with cooperative caching", *Ad Hoc Network, ELSEVIER, 7(3), 2009, 579-598.*

[5]. C.-Y. Chow, H. V. Leong, and A. T. S. Chan "GroCoca : Group-based peer-to-peer cooperative caching in mobile environment" *IEEE J. Sel. Areas Commun., 25(1), 2007, 179-191.*

[6]. X. Fan, J.Cao and W.Wu "Contention-Aware Data Caching in Wireless Multihop Ad Hoc Networks", *Proceeding of 6th International Conference on Mobile Adhoc and Sensor Systems, IEEE, 2009, 1-9.*

[7]. Y.-W.Ting and Y.-K. Chang, "A Novel cooperative caching scheme for wireless adhoc networks : GroupCaching", *International Conference on Networking, Architecture, and Storage (NAS), IEEE, 2007, 62-68.*

[8]. M.Fiore, C.Casetti and C.F.Chiasserini, "Caching Strategies Based on Information Density Estimation in Wireless Ad Hoc Networks", *IEEE transaction on vehicular tech., 60(5), 2011, 2914-2208.*

[9]. J. Cao, Y. Zhang, G. Cao, and L. Xie, "Data consistency for cooperative caching in mobile environments", *Computer 40(4), IEEE, 2007, 60-66.*

[10]. N. S. Fatima and P.S.A. Khader, "Enhanced Adaptive Data Cache Invalidation Approach for Mobile Ad Hoc Network*", Proceeding of international conference on Electronics Computer Technology, IEEE, 2011, 76-80.*

[11]. A Hamieh, J Ben-Othman, L Mokdad, "Detection of radio interference attacks in VANET", *Proceedings of the 28th IEEE conference on Global telecommunications, 2009, 5077-5081.*

[12]. Q Guan, FR Yu, S Jiang, VCM Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications". *IEEE Trans. Veh. Technol. 61, 2012, 2674-2685.*

[13]. F Dressler, F Kargl, J Ott, O Tonguz, L Wischhof, "Research challenges in intervehicular communication : lessons of the 2010 Dagstuhl seminar", *IEEE Commun. Mag., 49, 2011, 158-164.*

[14]. Li Zhu, F Richard, Bin Ning and Tao Tang, "A joint design of security and Quality of Services(QoS) provisioning in vehicular adhoc networks with cooperative communications", *EURASIP, Journal on Wireless Communication and Networking, 2013, 88-102.*

[15]. T. Heer, S. Gotz, O. G. Morchon, K. Wehrle, "ALPHA :An Adaptive and Light-weight Protocol for Hop-by-Hop Authentication", *Proceedings of ACM CoNEXT Conference , 2008, 210-222.*

[16]. G. Cao, "A Scalable Low-Latency Cache Invalidation Strategy for Mobile Environments", *IEEE Transactions. on Knowledge and Data Engg., 15(5), 2003, 1251-1265.*

[17]. P. Cao and C. Liu, "Maintaining Strong Cache Consistency in the World- Wide Web", *IEEE Transactions on Computers, 1998, 445-457.*