International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3S, February 2019

Secure Content Delivery with Cooperative Content Replacement in Mobile Networks

A.M. Resmi, R. Manicka Chezian

Abstract--- Mobile networks are fast growing, well adapted and more flexible. So, the content delivery network functionalities are more integrated with mobile networks. This will provide an optimal content oriented service for multimedia data sharing. In the request relaying and redirection process, traffic congestion can be caused in the base station. Congestion avoidance and load distribution are more important for effective mobile CDN (Content Delivery Networks). In this paper, a three-set of problems such as optimization problem of content placement, request redirection, and security issues are identified and rectified. To achieve this, we improved data delivery performance with security features over mobile CDN by deploying two new algorithms named as "Cooperative Content Placement Algorithm (CCPA) and Secure User Request Redirection (SURE)". The above two algorithms are incorporated into the Mobile Ad hoc Network (MANET) protocol and named as CSAODV. This overcomes the existing blind request redirection issues in mobile CDN, which contains the storage for replicating content. The simulation results show the performance of the proposed algorithms and achieved the secure stable data transformation over mobile CDN with low transmission cost.

Index Terms--- Content Delivery Networks, Mobile Networks, Data Distribution, Content Placement, User Request Handling.

I. INTRODUCTION

A content delivery network (CDN) works in a mechanism that the scattered servers (network) that deliver pages and other web content to a user [1]. These systems join by depending upon the factors such as geographic locations of the user, origin of the webpage, content delivery server. Websites that countenance with huge traffic at the global reach can exploit CDN, which proceeds with effectual rapidity of content delivery. Delivery of content to the user depends on the unfriendliness of the CDN server, to be precise closer the CDN server to the user geologically; delivering the content will be refined faster. Not only CDN delivers the content faster, but also affords to safeguard from large surges in traffic. The proposed work provides a scalable and secure content delivery in mobile CDN. To achieve, the proposed mechanism develops a new protocol named as CSAODV (Cooperative Secure Adhoc On demand Distance Vector). This includes **Cooperative Content Placement Algorithm (CCPA) and Secure User Request Redirection (SURE)** algorithms**.** The algorithms are used to achieve highly reliable and stable content delivery in the mobile CDN. The proposal assigns the user request to the proxy without any prior knowledge on the network attributes. The paper is organized as follows. The related and literature works on content caching and content distribution is summarized in section 2. Section 3 describes the proposed methodology and section 4 gives the results and discussion about the proposed work. The final section 5 concludes the proposed work and provides future directions.

1.1 Working of CDN

Response to the website visitor is acquired from the servers in close proximity to the website. By caching the contents of the page, the content delivery network will make a copy of the website pages to a set of connections to the servers which is discrete at the locality with poles apart geologically region. CDN follows the procedure of redirecting the user requests, at the circumstance when a user requests a webpage which is at present a part of a content delivery network. Transmitting the request is done to the actual site of the server in the CDN which is closest to the user and distributes the cached content. CDN's also works for the content which has not been cached beforehand. Users will be unacquainted regarding the commencements of CDN. User can recognize the accessibility of CDN, in case the URL (Uniform Resource Locator) delivered is dissimilar than the URL which has been necessitated.

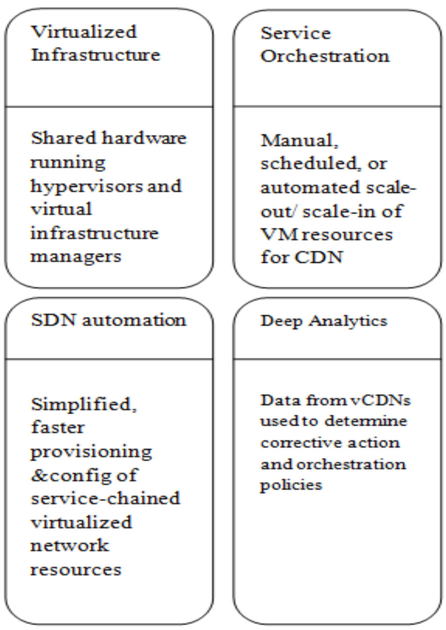

Figure 1: Pillars of Orchestrated CDN

Manuscript published on 28 February 2019.
***** Correspondence Author (s)
A.M. Resmi, Ph.D Research Scholar, Department of Computer Science, NGM College, (Autonomous), Pollachi, India.
(e-mail: resmiswararag@gmail.com)
Dr.R. Manicka Chezian, Associate Professor, Department of Computer Science, NGM College (Autonomous), Pollachi, India.
(e-mail: chezian_r@yahoo.co.in).

CDN servers enhance the working method by decreasing the latencies, hastening site load times, reducing bandwidth usage by providing securities and also obstruct data scrappers and other forms of spammers striking the server for the case of transmitting large scale websites to global spectators. Content delivery plays a vital role in B2B (Business 2 Business) interactions in order to dole out the consumers. Because of increasing daily-life with online budge, concerns access to content delivery network to speed up with static content, dynamic content, mobile content, e-commerce contracts, etc [2].

Challenges in CDN

The challenges faced in CDN are Capacity Planning – Anticipating Demand, Agility – Responding to Demand, Cost – Consolidating Delivery, Quality – Optimizing Delivery.

Capacity Planning- Anticipating Demand: Primitive methods define the competence of CDN when it is been owed on variables such as the volume of bandwidth, number of spectators in a specific topography, along with the cumulative byte volume of delivered content. Furthermore, add-on ability is the pre-condition to hold spikes in consumption. Over-provisioning leads to wasted resources.

Agility- Responding to Demand: Among the flanked erection process for new servers, the total time required to construct and deliver servers, the inclusion of the exertions necessary to install and constitute the software to the server may finish in stiffing out CDN in weeks or even months.

Cost- Consolidating Delivery: Prospectively, over-spend on the CDN's ability is waste. Moreover, the make-out of each and every distinct objective communication for the entire services can encumber and very expensive for the network operators. It is sometimes thorny to predict their requirements. Purpose-built servers, a type of a system which has been implying to endow the usage for one type of service has the chances to execute well but also have some limitations, in other cases.

Quality- Optimizing Delivery: CDN's are deployed in superior central and local data centers as conflicted to very small points of presence (Pops). For centralized loom, the libraries with bulky content will be accomplished. In favor of such higher-audience events, the famous live linear content has found to be superior proficient to deliver from CDN resources which are positioned in small PoPs deeper network.

The proposed work presents the critical issues involved in designing and implementing an effective Mobile CDN and proposed a new approach to address these problems. Authors Vakali et al in [1] presented a survey of CDN architecture and the list of popular CDN service providers, from the article the CDN architecture is clearly identified. The authors have identified the features of the content network domain and the trends in CDN, from that analysis, the proposed work initiated an optimized taxonomy for mobile CDN. It can identify the characteristics and current practices in the content networking domain, and present an evolutionary pathway for CDNs, in order to exploit the current content networking trends. There are a huge set of CDN providers provides efficient and reliable data delivery services. The popular CDN service providers are Akamai, MaxCDN, Rackspace, etc.,. These service providers offer various services to satisfy user needs to improve service ratings and helps to adopt mobile user's requests. The aim of the proposed work is to provide highly reliable content delivery services to mobile users. The paper is organized into different chapters such as literature work on mobile CDN, the proposed system and its methodology, the next chapter gives the results attained from the simulation.

II. LITERATURE SURVEY

Yousaf*et al.* [3] consider the deployment of a mobile CDN system in the 3GPP network to ensure a fair delivery of progressive video streaming services. The unfairness issue when delivering progressive video streaming services over TCP to multiple users over a wireless network infrastructure, this information are first highlighted by Authors. Authors then demonstrate, as a proof of concept, the effectiveness of employing application-level scheduling in anmCSP node to ensure fairness among multiple simultaneous progressive video sessions in scenarios where the backhaul link in a mobile network infrastructure may become congested. Challenges for research and implementation remain in the concrete design of algorithms that gain advantage from control plane information. These include the generation of congestion-topology graphs, as well as the identification and treatment of content delivery, flows that traverse a congested region, as well as how to derive QoE for progressive video streaming from limited input or development of appropriate fairness metrics for QoE.

Liebsch and Yousaf [4] show the benefits of having CDN serving points for mobile content delivery in terms of transmission cost saving. In this paper, authors motivate the support of runtime CDN Serving Point relocation to keep mobile content delivery costs independent of the mobile devices' mobility patterns. The contribution aims at the description of suitable technology serving as building blocks for the design of a complete solution for runtime CDN Serving Point relocation and to substantiate the feasibility of the proposed solution. These building blocks comprise technology for IP traffic offload in cellular mobile communication networks and IP address continuity in distributed mobility management, as well as socket and application context migration as an enabler for runtime CDN serving point relocation. The focus of the paper was on a simulative study to show the gain in saving transport costs during mobile content delivery. In the modeled network topology, savings of up to 65% of content delivery costs from content caches in the network's aggregation network have been achieved in a system with enabled runtime relocation support.

Almashor*et al.* [5] studied the CDN mechanisms onto mobile platforms by exploring the storage capacities of mobile devices, and they address a content replication problem. The concept of a CDN given by mobile-devices is novel.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Considering their growing presence and capabilities, it is reasonable to expect smart-phones, tablets, and laptops to drive forward the next generation of CDNs. In this work is proposed the utilization of highly transient wireless devices like servers, and aims to improve service speed via replication. This method helps to determine file availability is provided, along with an effective way to manipulate replica numbers so as to minimize service times. The experimentation results are promising. Future areas of study include the use of the models in a global network. The work is considered assumes a small wireless cluster as a single replication container. Beyond the cluster confines, it would be interesting to see the mechanism recursively applied to higher network levels.

Boskovic*et al.* [6] investigate the energy efficiency aspect of a CDN system based on Mesh WiFi implementation. However, few of these works address the implementation of a CDN by leveraging the storage capacities of BSs although the recent efforts at ETSI MEC, in particular, related to NFV, go into this direction. In this paper, authors have investigated the energy efficiency of a special class of video CDN system, namely pervasive wireless CDN based on Mesh Wi-Fi implementation. Both analytical calculations and computer simulations confirmed the initial hypothesis that content placement strategy for a wireless CDN has to carefully balance energy consumption vs. QoS/latency performances. Authors have captured the idea of intelligent coordination of content placement among wireless access points that serve as edge video servers into a number of experiments, applied computer simulation based on mixed integer linear programming (MILP) model and demonstrated its capability to come up with "optimal" content placement and caching strategies as function of power consumption and QoS requirements. The analytical approach has shown a very strong dependency between the energy efficiency for this class of CDNs and associated content hit ratio. This all points out towards very strong need to build context driven wireless video delivery networks in which content/caching placement strategies are dynamically changed in accordance with user's request changes, user's mobility, content popularity. As video consumption on wireless portable devices is growing rapidly the vision presented here is to get closer to being practically deployed in a form of pervasive wireless CDN in which extra storage resources are added to the wireless access points in order to enable mesh router offers local video server functionalities. In that scenario, the established dependencies between the quality of service and energy consumption will prove to be a valuable resource to future wireless CDN designer and/or network managers.

2.1 Content Caching System

Ashleigh and SujitDey [7] propose reactive caching policies for BS caching system to reduce traffic throughput on backhaul links. Authors also implemented caches on small cells to mitigate traffic pressure on backhaul links. The study solved the issues in achieving the optimum content placement problem. At last, the total file downloading time is reduced. Borst*et al.* [8] authors designed and developed algorithms to allocate storage capacity for one content in a mobile network with cache-enabled BSs. They show that the complexity of the content placement problem is NP-Hard. NP hard problem is a decision-making problem, which is handled by the high effective cache enabled base stations. Authors investigate content replacement strategy on BS cache. The problem is modeled by a Markov decision process, and a distributed content placement algorithm is proposed.

Collaborative caching of traditional wired CDN systems. In collaborative caching, joint optimization of content placement and user request redirection has been studied in a number of works. The problem is known as NP-Hard. He *et al.* [9] consider both problems separately at different time scales to reduce the problem complexity. Applegate *et al.* [10] jointly address the content placement and request redirection problem, subjects to storage capacity, and link bandwidth. However, the problem complexity prevents a fast efficient solution.

Despite the use of exponential potential function methods, it still takes a long time to find a sub-optimum solution, which prevents its implementation in a dynamic environment. Borst*et al.* [11] study the joint problem in a hierarchical tree structure. The problem is solved optimally in a certain simplified scenario. For general scenarios, a greedy content placement algorithm is proposed. Amani*et al.* [12] formulate the joint optimization problem to minimize content access delay in a general CDN architecture, and two heuristic algorithms are proposed.

For the comparison, the AODV (Adhoc On demand Distance Vector), AOTDV (adhoc on demand trusted path distance vector) and SAODV (secure Adhoc On demand Distance Vector) [13] have used. This protocol taken for comparison and this is incorporated with the existing content placement and security algorithms.

III. PROBLEM DEFINITION

These existing works devise the joint content placement and request redirection schemes based on statistical network environment parameters, such as content popularity, transmission cost or link capacity. As a result, they cannot cope with system dynamics. Moreover, evaluating and collecting statistical information about mobility and content popularity is difficult in practice. Some proposals rely on known parameter distribution (such as dynamic programming). However, the distribution of these parameters can vary (for instance, the distribution of content popularity can change).

IV. PROPOSED SYSTEM

Providing CDN services into the mobile network is called a MobileCDN system. In this type of network, CDN and mobile networks have common features to concatenate on the applications. This integration improves the quality of service to multimedia content streaming services because multimedia streaming services always require low latency and network stability.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The MobileCDN reduces the communication and transmission cost by mitigating the traffic issues on the mobile core networks. The special storage unit on the base station allows the mobile CDN to replicate the content and reply when it is requested from a mobile user. The MobileCDN have different types of issues like content selection and replacement and user request redirection. These issues are always coupled together and affect the overall performance of the content distribution process. Content replacement and request redirection issues have already discussed in the literature. These work aims to avoid the joint optimization problems in the content replacement issue. But, the transmission capacity of replying caches is ignored. The user requests are redirected to the high probability cache based on the availability. This navigation generates high traffic and high workload for the mobile base stations. While comparing the caches in the wired network with the wireless network, wired caches are powerful and good in performance. Congestion avoidance and performance issues are handled in the mobile CDN. In this paper, a new optimized mechanism is proposed to overcome the congestion issues and performance related issues in MobileCDN. The mechanism concentrates on the cooperative content replacement, optimal user request redirection and secure content delivery in MobileCDN. The proposed mechanism develops a new **Cooperative Content Placement Algorithm (CCPA) and Secure User Request Redirection (SURE)** algorithm**.** The algorithms are developed to achieve highly reliable and stable content delivery over mobile CDN. The proposal assigns the user request to the proxy without any prior knowledge on the network attributes.

4.1 Proposed system Framework

The system proposes a new base station based mobile CDN system, which provides optimal and cooperative content replacement and effective secure user request redirection. The content delivery network consists of several base stations and equipped with the storage unit. The remote server emits content to the base station and base station performs the content fetching from various and multiple base station. This content pre-fetching and caching concepts improve performance. The user request redirection with security metrics is formulated in the proposed work.

The secure content replacement and user request redirection in MobileCDN has been developed using two new algorithms. In the overall process, a mobile user sends content requests to the attached BS. The BS checks whether the requested content is stored. In case of a miss, the request is redirected to another BS in the system. A remote CDN origin server, noted as *n*0, can eventually provide the requested content in some of the cases such as, when the requested content is not available in BSs, When the transmission cost to get the content from the remote server is lower than from the candidate BSs and When the BSs backhaul uplink endures heavy traffic congestion. The proposed infrastructure is a dynamic one, where the system contains a set of times slots with the index values t. different attributes and parameters are used in a different situation. This includes the position of the requested users, the received content requests and the status of traffic. But the main drawback of this is, it limits the changing process in every time slot. The pre-specified time slots activities are unpredictable. Because the client request in mobile networks is always unpredictable. So, the proposed system developed a new set of algorithms such as Cooperative Content Placement Algorithm (CCPA) and Secure User Request Redirection (SURE)". This initiates the user request.

Cooperative Content Placement Algorithm (CCPA) and Secure User Request Redirection (SURE):

The complexity of content placement in mobile CDN comes from the joint optimization of and request redirection. There is a method is used to reduce the complexity of the joint problem, which is segmented into an ensemble. One method to reduce complexity is to decompose the joint problem into the content placement subproblem and request redirection sub-problem, and to solve these two subproblems separately. By observing the structure of the problem, we decompose it into two separate parts. First, a content placement subproblem determines a content replication which coincides with an upper bound on transmission cost. Then, based on the resulting content placement and data request service, a request redirection subproblem finds the minimum transmission cost for the specific setting. Then, we introduce CCPA, a cooperative content placement algorithm, which decides the content placement and request redirection for each time slot based on the server updates. The following notations are used in the algorithm.

Notations:

- n0 –CDN origin server
- N-total number of Base stations
- T-time slot
- index value t

Algorithm 1 Content Placement Algorithm for Each Time Slot

1: CP part: solving Problem (P3):
2: Each BS sends user requests *{dki }*to the CP.
3: CP solves Problem (P3) through LGAP algorithm.
4: CP sends storage decision messages to BSs.
5: BS part: practical improvement:
6: ∀BS *ni*, cache content indicated in the decision message.
7: *list i* ← not cached content.
8: Sort *list i* in *lki* decreasing order.
9: Store content in *list i* until no capacity.

The mobile network operators are very interested in Integrating CDN functionalities into the mobile network so enhance their capability for supporting the content-oriented services; these all improvements are gathered by the development of network function virtualization and SDN (Software-defined networking) standards. Considers of a *mobile CDN* system, where Base Stations (BSs) are equipped with replicating contents storage area. In the system give some tasks such as BSs cooperation in replying user requests through backhaul links is a widely adopted mechanism. If sometimes blindly redirect user requests upon content placement can cause traffic congestion.

As a result, congestion avoidance and load balancing is an important issue to be tackled in this scenario. The concept investigation provides the joint optimization problem of content placement and request redirection for the BS-based mobile CDN. Particularly, each BS maintains a transmission queue for replying requests issued from other BSs. Traffic Congestion or Network congestion and BSs load balancing can be jointly considered through guaranteeing network stability. In this analyzation gives the *stochastic optimization model* to minimize the long-term time-average transmission cost under network stability constraints. By using the Lyapunov optimization technique, we transform the long-term problem into a set of linear programs solved at every time slot duration, and we develop a cooperative secure data caching algorithm. In this algorithm is efficiently decides the content placement and request redirection without requiring *a priori* knowledge on the random network state information. Via the simulation analysis, the performance of the algorithm on optimality and network stability is given. The evaluation confirms that the solution can achieve low transmission cost, whilst avoiding congestion and balancing traffic loads.

The main function of the **Secure User Request Redirection** algorithm is to allow only the legitimate packets and deny the attack packets in the content distribution. This is done based on the white listed and malicious IP addresses. In this process, the Nodes in the network are clock synchronized, and with no network failure. And the time stamp is enabled in the packets. For a secure data caching and content transmission SURE us used. This refers to generating the vertices in the signature graph and inserting them into the encode table (ET). Each path from the BS to the client has a signature and each node in the path has its unique node id (N_{ID}). A path is uniquely identified for every transaction by the SURE. The SURE is generated per-transaction based on the packet sequence number (Pq) and the N_{ID}. We use SURE algorithm For N_{ID} generation. And this will be secured. Thus for a given data packet for selected BS, the secure content transmission is performed as,

$$\text{SURE-}N_{ID}=S(\text{generateID}(N_{IDi},Pq)) \quad \text{Equation(1)}$$

Where S is the Security block chipper function, when a BS generates a packet, it also creates a timestamp value Ts of the Nid and appends in the packet header. The source then generates a content distribution and cache according to Equation (1), inserts the SURE-N_{ID} into ET and transmits the Ts as a part of the packet. Upon receiving the data from the BS, each node performs data transmission and verification of other cache nodes. If the node is valid node and if itsN_{ID} are in the header, then the Tid value will be updated with the least bit value. At the time of verification the prototype verifies the previous SURE-N_{ID}based on the N_{ID} at every node.

V. EXPERIMENTAL RESULTS

The proposed CSAODV is implemented in MCDN and compared with AODV to investigate the performance of the proposed method. The proposed CSAODV method was implemented for MCDN and the simulation results were obtained for the proposed method of attacker detection and isolation.The following metrics namely Packet delivery ratio, routing overhead, End-to-end delay, False positive ratio and Detection time is used to evaluate the performance of the proposed method.

5.1 Performance analysis on the percentage of attacker nodes

The performance of the proposed method was evaluated with respect to packet delivery ratio, end-to-end delay and routing overhead for various percentages of attacker nodes in MANET. The proposed method improves the packet delivery ratio, reduces the end-to-end delay and reduces the routing overhead.

a) Performance in terms of packet delivery ratio

The number of network nodes and the flows was fixed at 200 and 50 respectively. The node mobility was set at 20m/sec. The simulation time was 300 seconds. The attacker nodes were stimulated in the network such that 2% of the nodes were attacker nodes. The packet delivery ratio was obtained for AODV, AOTDV, SAODV, and CSAODV. Similarly, the packet delivery ratio was obtained for AODV, AOTDV, SAODV, and CSAODV in the MANET having 4%, 6%, 8% and 10% of nodes as attacker nodes separately. The results are given in figure 2.

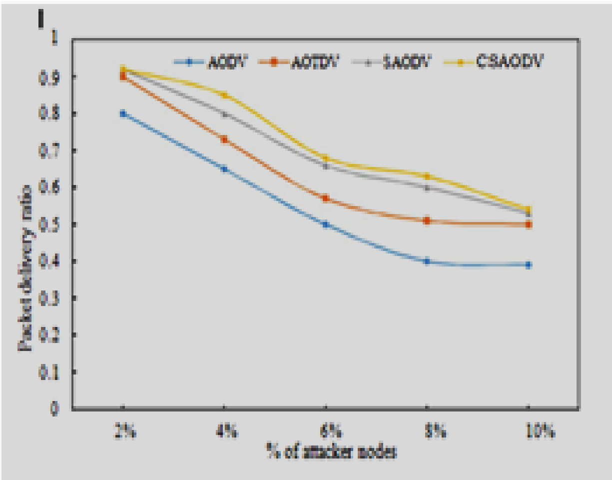

Figure 2: Percentage of attacker nodes vs. Packet delivery ratio (CSAODV)

It is evident from fig 7 that the packet delivery ratio of CSAODV is higher than the other protocols. CSAODV shows 3.04% improvement in packet delivery ratio. This is due to the fact that the attacker nodes are identified and isolated from the MCDN quickly. Hence, the data traffic is routed only through legitimate nodes. The delivery ratio of AOTDV is higher than AODV because in AOTDV the intermediate nodes have redundant routes to the destination. This provides a way for legitimate nodes to perform their normal operation. In addition, the isolation of the attacker node causes a transient network partition. Hence, the packet delivery ratio decreases for every increase in the percentage of attackers.

b) Performance in terms of routing overhead

The behavior of the protocols in terms of routing overhead was investigated.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The number of network nodes was 200.

The number of flows was fixed at 50. The simulation time was set at 300 seconds. The node mobility was 20m/sec. The attacker nodes were stimulated in the MCDN. Initially, the percentage of the attacker nodes was set at 2% of the nodes in the MCDN. The routing overhead was obtained for AODV, SAODV, and CSAODV. The results are shown in fig 8. Similarly, the routing overhead was obtained for them in the MCDN having 4%, 6%, 8% and 10% of nodes as attacker nodes separately. The results are shown in figure 3.0. The results show that even when 10% of the MCDN nodes were attacker nodes, routing overhead of CSAODV is much lower than the AODV protocol.

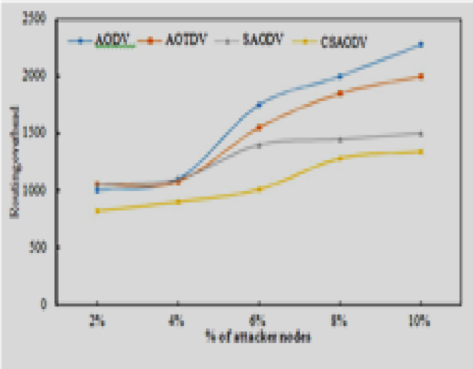

Figure 3: Percentage of attacker nodes vs Routing overhead (CSAODV)

This is primarily because CSAODV detects and isolates the attacker nodes quickly thereby reducing the packet loss in the network. As a consequence, the necessity of routing packets is considerably reduced by 4%. Further, the proposed CSAODV methodology does not demand any additional routing messages whereas SAODV requires additional one hop RREQ messages to be broadcasted for the identification of the attacker nodes.

c) Performance in terms of end-to-end delay

The behavior of the protocols in terms of end-to-end delay is analyzed. The number of network nodes was 200. The number of flows was fixed at 50. The simulation time was 300 seconds. The node mobility was 20m/sec. The attacker nodes were stimulated in the MCDN. Initially, the percentage of the attacker nodes was set at 2% of the nodes in the MANET. The end-to-end delay was calculated for AODV, AOTDV, SAODV, and CSAODV. Similarly, the end-to-end delay was obtained for these methods in the MCDN having 4%, 6%, 8% and 10% of nodes as attacker nodes separately. The results are shown in figure 4.0.

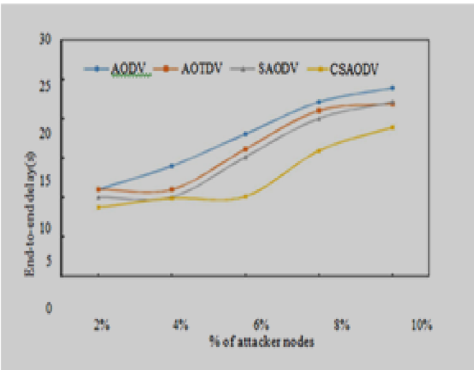

Figure 4: Percentage of attacker nodes vs End-to-End delay (CSAODV)

The end-to-end delay exhibited by CSAODV is 7.96% lower than SAODV. This is due to the fact that CSAODV protocol isolates the attacker node from the MCDN immediately causing the routing table entry invalid. Hence, the routing protocol requires to initiate a route discovery process for finding out the new routes to the destination. Hence, the end-to-end delay increases with the increase in the percentage of attacker attackers. In AOTDV, before the routing information is updated in the routing table, the new routes are stored in the secondary cache. After the verification of the legitimacy of the routes, they are added to the routing table. This causes the end-to-end delay to be higher for AOTDV.

d) Performance in terms of the false positive ratio

To investigate the accuracy of the proposed methodology in detecting the attacker node in the MCDN, the false positive ratio is calculated. The attacker nodes were stimulated into the MCDN and the percentage of the attacker was increased by 2% and the number of attacker nodesis identified. The false positive ratio of AOTDV, SAODV and CSAODV were calculated and shown in figure 5.

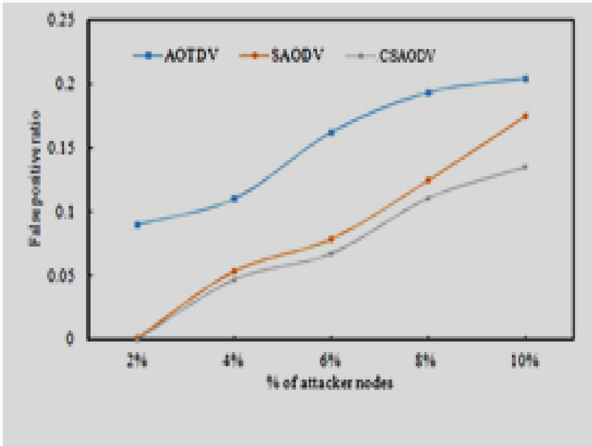

Figure 5: Percentage of attacker nodes vsFalse positive ratio (CSAODV)

The false positive ratio of the proposed CSAODV method is very less when compared to the existing methodologies. The false positive ratio is reduced by 16.8% for CSAODV in comparison with other methodologies.

e) Performance in terms of detection time

To investigate the time taken for the proposed methodology to detect the presence of the attacker nodes, the detection time is calculated. The detection time is calculated for AOTDV, SAODV, and CSAODV for various percentages of attacker nodes in the MCDN. The output is shown in figure 6. It is observed that the detection time of CSAODV is very less in comparison with the other methodologies. The detection time of CSAODV is reduced by 14.45% when compared with other methodologies.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

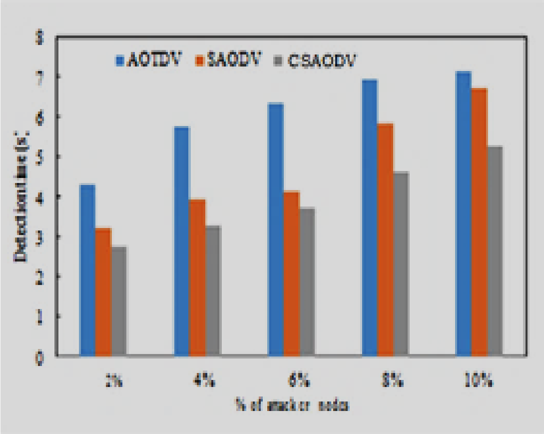

Figure 6: Percentage of attacker nodes vs Detection time (CSAODV)

VI. CONCLUSION

Mobile networks are widely developed to provide optimal content oriented service for multimedia data sharing in the recent scenario. In the request relaying and redirection process, traffic congestion can be caused in the base station. While delivering the contents, Congestion avoidance and load distribution are more important for effective mobile CDN. In this paper, a three-set of problems such as optimization problem of content placement, request redirection, and security issues are identified and rectified in the mobile CDN. In the mobile CDN, set new algorithms are implemented in a protocol and the protocol is called as CSAODV (Cooperative secure ad-hoc on demand distance vector) for Mobile CDN. This includes algorithms such as "**Cooperative Content Placement Algorithm (CCPA) and Secure User Request Redirection (SURE)**". The simulation results and the performance graphs are plotted and that shows the performance of the CSAODV and achieved the secure stable data transformation over mobile CDN with low transmission cost and high attack detection ratio.

REFERENCES

1. Pallis, George, and Athena Vakali. "Insight and perspectives for content delivery networks." Communications of the ACM49.1 (2006): 101-106.
2. Pathan, Al-Mukaddim Khan, and RajkumarBuyya. "A taxonomy and survey of content delivery networks." Grid Computing and Distributed Systems Laboratory, University of Melbourne, Technical Report 4.0 (2007):
3. Yousaf, FaqirZarrar, et al. "Mobile CDN enhancements for QoE-improved content delivery in mobile operator networks." IEEE Network 27.2 (2013):
4. Liebsch, Marco, and FaqirZarrarYousaf. "Runtime relocation of CDN serving points-enabler for low costs mobile content delivery." 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2013.
5. Almashor, Mahathir, et al. "Enhancing availability in content delivery networks for mobile platforms." IEEE Transactions on Parallel and Distributed Systems 26.8 (2015): 2247-2257.
6. Boskovic, D., FaramakVakil, StanišaDautovic, and M. Tosic. "Greening of video streaming to mobile devices by pervasive wireless CDN." Journal of Green Engineering (2) (2011): 1-27.
7. Ahlehagh, Hasti, and SujitDey. "Video-aware scheduling and caching in the radio access network." IEEE/ACM Transactions on Networking (TON) 22.5 (2014):
8. Borst, Sem, Varun Gupta, and Anwar Walid. "Distributed caching algorithms for content distribution networks." 2010 Proceedings IEEE INFOCOM. IEEE, 2010.
9. He, Jun, Honghai Zhang, Baohua Zhao, and SampathRangarajan. "A collaborative framework for in-network video caching in mobile networks." arXiv preprint arXiv:1404.1108(2014).
10. Applegate, David, et al. "Optimal content placement for a large-scale VoD system." Proceedings of the 6th International COnference. ACM, 2010.
11. Borst,Sem,VarunGupta,andAnwarWalid."Distributed caching algorithms for content distribution networks." 2010 Proceedings IEEE INFOCOM. IEEE, 2010.
12. Amani, Payam, SaeedBastani, and Bjorn Landfeldt. "Towards optimal content replication and request routing in content delivery networks." 2015IEEE International Conference on Communications (ICC). IEEE, 2015.
13. Karande, Hema R., and Sandeep A. Thorat. "Performance analysis of FTDSR and AOTDV trust based routing protocols." 2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN). IEEE, 2014.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)