Volume 8, Issue 4
August 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Effective DDOS Attack Detection with Input Data to Different Customer and Multi Personal Model

[1]R. Nandhini and [2]Dr. A. Banumathi
[1]PG and Research Department of Computer Science, M.Phil., Scholar, Govt. Arts College, Karur
[2]PG and Research Department of Computer Science, Assistant Professor,
Govt. Arts College, Karur
E-mail: [1]nandhurose30@gmail.com

ABSTRACT

Data Outsourcing issues were monitored, where a trusted server is in charge of defining and enforcing access control policies in vehicular ad-hoc network VANETs. The main scope of this paper is used to deliver the necessary data for the third party based on demand access. The user access the details on privilege level based on access control in VANET. The dual encryption is processed in the network environment which is varied from one group to another for secure data transmission process. The algorithm namely Local flow and QOD Routing algorithm to enforce access control policies with user revocation capability. a novel traceback with method for DDoS attacks detection using Local flow and QOD Routing algorithm. QOD Routing algorithm based on different customer data and multi personal model analysis. The DDOS attack traffic analysis using entropy variations between normal and different from commonly used packet marking techniques. In comparison to the existing Local flow traceback methods, the proposed QOD strategy possesses a number of advantages-it is memory non-intensive, efficiently scalable, robust against packet pollution, and independent of attack traffic patterns. The results of extensive experimental and simulation studies are presented to demonstrate the effectiveness and efficiency of the QOD method with customer multi personal model.

Keyword: *VANET, Data Sharing Scheme, DDOS attack, Trace back, Local flow, QOD protocol*

1. INTRODUCTION

DDOS A novel DDOS attack detection scheme Footprint, using the trajectories of vehicles for identification while still preserving the anonymity and location privacy of vehicles. Specifically, in Footprint, when a vehicle encounters an RSU, upon request, the RSU issues an authorized message for this vehicle as the proof of its presence at this RSU and time. Intuitively, authorized messages can be utilized to identify vehicles since vehicles located at different areas can get different authorized messages.

However, directly using authorized messages will leak location privacy of vehicles because knowing an authorized message of a vehicle signed by a particular RSU is equivalent to knowing the fact that the vehicle has showed up near that RSU at that time. In Footprint, to design a location-hidden authorized message generation scheme for two purposes. First, RSU signatures on messages are signer-ambiguous which means an RSU is anonymous when signing a message.

In this way, the RSU location information is concealed from the final authorized message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same RSU are recognizable if and only if they are issued within the same period of time. Thus, authorized messages can be used for identification of vehicles even without knowing the specific RSUs who signed these messages. With the temporal limitation on the link ability of two authorized messages, authorized messages used for long term identification are prohibited. Therefore, using authorized messages for identification of vehicles will not harm anonymity of vehicles.

2. RELATED WORKS

U. Jyothi K et al., [1] summarizes for which resources of the computing infrastructure are provided as services over the Internet. This paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. The aim to keep the data confidential against untrusted server's cryptographic methods may be applied by disclosing data decryption keys only to authorized users. However, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well.

Brent Waters et al., [2] describes a public- key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share a targeted user or device. While this is useful for applications where the data provider knows specifically which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user's credentials. In the techniques provide a framework for directly realizing provably secure CP-ABE systems. The encrypted text distributes shares of a secret encryption exponent s across different attributes according to the access control LSSS matrix M. A user's private key is associated with a set S of attributes and he will be able to decrypt an encrypted text if his attributes "satisfy" the access matrix associated with the encrypted text.

During decryption, the different shares that the algorithm combines are multiplied by a factor of the ultimately these randomized shares are only useful to that one particular key. To construct a structures and high level intuition for security is similar to the BSW construction. The main novelty in the paper is provided a method for proving security of such a construction.

Dan Boneh et al., [3] describe Identity Based Encryption (IBE) system where the public key can be an arbitrary string such as an email address. A central authority uses a master key to issue private keys to identities that request them. The first construction for HIBE is due to where security is based on the Bilinear construction due to Boneh and Boyen gives an efficient (selective-ID secure) HIBE based on BDH

without random oracles. The length of cipher-text and private keys grows linearly in the depth of the hierarchy. There are currently two principal applications for HIBE.

VipulGoyal et al., [4] describe a more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites One issues handled in this paper is encrypting the data that would be selectively shared only at a coarse-grained level (i.e., giving another party private key). Develop a new cryptosystem for fine-grained sharing of encrypted data that they call Key-Policy Attribute-Based Encryption (KP-ABE). In the cryptosystem, encrypted text are labeled with sets of attributes and private keys are associated with access structures that control which encrypted text a user is able to decrypt. Demonstrate the applicability of construction to sharing of audit-log information and broadcast encryption.

Michael Armbrust et al., [5] concentrates the illusion of infinite computing resources available on demand, thereby eliminating the need for Cloud Computing users to plan far ahead for provisioning. The elimination of an up-front commitment by Cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs. The cloud users need to pay for use of computing resources on a short term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

3. DDOS ABE Model

The working algorithm logic in encryption is ABE comes in two flavors called Key-Policy ABE (KP-ABE) and cipher text policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into user's keys; while in CP-ABE, the attributes are used to describe a user's credential, and an encryptor determines a policy on who can decrypt the data's-ABE is more appropriate to the data outsourcing architecture than KP-ABE because it enables data owners to choose an access structure on attributes and to encrypt data to be outsourced under the access structure via encrypting with the corresponding public attributes.

While encrypting the confidential data, there may introduce several challenges with regard to the attribute and user revocation. The revocation issue is even more difficult especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, it refer to such a collection of users as an attribute group). It also defines the affect due to the revocation of users from the group. It may result in bottleneck during re-keying procedure or security degradation in the system.

The existing system depending full of manual process, manual system maintains the limited number of process. The existing system includes an attribute-based access control scheme using CP-ABE with efficient attribute and user revocation capability for data outsourcing systems. The existing system consists of the following entities:

The authorized person will generates public and secret parameters for issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on the attributes. It is the only party that is fully trusted by all entities participating in the data outsourcing system.

Server who outsources data to the external data server provided by the service provider is termed as data owner. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before outsourcing it. The one who access the outsourced data will be known as user. If user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then the user will be able to decrypt the encrypted text and obtain the data.

Security Service Provider consists of data servers and a data service manager. The cloud service provider is in charge of controlling the accesses from outside users to the outsourced data in servers and providing corresponding contents services. The following are the drawbacks of DDOS attack system:

1. Handling the outsource data copies in a secure manner is difficult.
2. Storing and retrieving of data from cloud server takes more time and effort.
3. The data owner need to take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation.
4. All the data is maintained by single service provider so the data privacy may be affected by the third party storage area.
5. Keys are assigned randomly and independently from each other, so the user can access the data of another user group by the system.
6. No capability to capture a series of attribute queries option.
7. User profile is group into single group attribute in the tuples structure only.
8. Past query based suggestion is not given to user group.

Below mentioned are the main objectives of the proposed system:

9. User can be revocated from particular group. After revocation, key assigned to the revocated user will be redefined and reused for another new user.
10. To maintain data servicing by more than one service provider.
11. To make all data service managers take charge of managing the attribute group keys per each attribute group.
12. To assign keys based on uniqueness among all users.

4. DDOS ATTACK MODEL

In DDOS attack system, first, enabling user access control enhances the backward/forward secrecy of outsourced data on any membership changes in attribute groups compared to the attribute revocation schemes. Second, the user access control can be done on each attribute level rather than on system level, so that more fine-grained user access control can be possible. In practical scenarios, users may miss many key update messages so that it cannot sometimes keep the key states up-to-date. This is called stateless receiver problem. In the proposed scheme, rekeying in the attribute group is done with a stateless group key distribution mechanism using a binary tree. This alleviates the scalability problem and resolves the stateless receiver issue.

Third, data owners need not be concerned about any access policy for users, but just need to define only the access control policy for attributes as in the previous DDOS attack system. The main objective of the DDOS attack system is to reduce the

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

time consuming and make the system more user friendly, efficient, accurate and fast process. The primary objective of the proposed DDOS system:

- To relocate users by any service provider may if unauthorized user tries to access the data above a given count.
- To maintain data servicing by more than one service provider.
- To make all data service managers take charge of managing the attribute group keys per each attribute group.

The DDOS system implements all the existing system concepts in which the encrypted text-Policy Attribute-Based Encryption with User Revocation is carried out. Like existing system, the proposed scheme also adapts a dual encryption approach to overcome the user access control problem in attribute-based encryption system. In addition, multiple service providers are included and data is distributed among them. User privileges may be varying for data maintained by different service providers. This requires different kind of encryption mechanisms in data maintained by different service providers. The following are the advantages of proposed system:

- Any cloud service provider may revocate users if unauthorized user tries to access the data above a given count.
- Data service is maintained by more than one cloud service provider, the authentication process is enhanced.
- Keys are assigned based on a condition and unique among all users, so the key duplication is not occurred in the current system.
- Handling the outsource data copies in a secure manner is easy to compare proposed attribute access control model.
- To capability and capture a series of attribute queries option.
- User profile is group into same group with attribute in the tuples structure only.
- Past query based suggestion is given to user group.
- All the data is maintained by multiple service providers so the data privacy do not affected by the third party storage area.
- The single data service manager is in-charge of managing the different attribute group keys per each attribute group

Attribute group key generation form is used to create group key in the application, attributes assigning with the group, identify each user belonging to the given group id. The attribute identity number is selected by the user in the checkbox control. Group identity number is inserted in the textbox control. All these details are saved in the specified table.

- This first phase is used to assign the user to group, for accessing the given process. The user identity number is selected by user.
- This next phase is used to encrypt the key value for corresponding username and user id.
- This next phase is used to encrypt the text using public key for the purpose of other users who do not know the given message.
- This next phase, re-encrypt the encrypted data in the application based on the group key because the other user will not identify the same encrypted message.

Decrypt cipher text retrieves the plain data in the application. The given cipher text is entered the data is showed to the user. This last phase is used to create cipher text in this experimental system given database the user access the high privileged level or not.

5. DIFFERENT CUSTOMER INPUT DATA AND MULTI PERSONAL MODEL

Customer different and multi personal model with intruders on the Internet often launch network intrusions indirectly, in order to decrease their chances of being discovered. One of the most common methods used to evade surveillance is the construction of stepping stones. In a stepping-stone attack, an attacker uses a sequence of hosts on the Internet as relay machines and constructs a chain of interactive connections using protocols such as Telnet or SSH. The attackers type's commands on his local machine and then the commands are relayed via the chain of "stepping stones or Local Flow" until they finally reach the victim. Because the final victim only sees traffic from the last hop of the chain of the stepping stones, it is difficult for the victim to learn any information about the true origin of the attack. The chaotic nature and sheer volume of the traffic on the Internet makes such attacks extremely difficult to record or trace back.

A. Local Flow

A Local Flow monitor analyzes correlations between flows of incoming and outgoing traffic which may suggest the existence of a stepping stone. Like previous approaches, we consider the detection of interactive attacks: those in which the attacker sends commands through the chain of hosts to the target, waits for responses, sends new commands, and so on in an interactive session.

Such traffic is characterized by streams of packets, in which packets sent on the first link appear on the next a short time later, within some maximum tolerable Delay bound Δ. The detection of non-interactive connections (i.e., those without a maximum delay Bound Δ) is much harder, as there is no bounded time frame within which packets on different streams need to compared. Like previous approaches, we assume traffic is encrypted, and thus the detection mechanisms cannot rely on analyzing the content of the streams.

However, most previous approaches in this area are based on ad-hoc heuristics and do not give any rigorous analysis that would provide provable guarantees of the false positive rat e or the false negative rate. The proposed method based on wavelet transforms to detect correlations of streams, and it was the first work that performed rigorous analysis of their method. However, they do not give a bound on the number of packets that need to be observed in order to detect attacks with a given level of confidence. Moreover, their analysis requires s the assumption that the packets on the attacker's stream arrive according to a Poisson or a Pareto distribution in reality, the attacker's stream may be arbitrary. Wang and Reeves proposed a watermark-based scheme which can detect correlation between streams of encrypted packets. However, they assume that the attacker's timing perturbation of packets is independent and identically distributed (iid), and their method breaks when the attacker perturbs traffic in other ways

Explicitly set our objective to be to distinguish attacking

pairs from non-attacking pairs, given our fairly mild assumptions about each. In contrast, the work of detects only if a pair of streams is correlated. This is equivalent to our goal if one assumes non-attacking pairs are perfectly uncorrelated, but that is not necessarily realistic and our assumptions about non-attacking pairs will allow for substantial coarse-grained correlation among them. For example, if co-workers work and take breaks together, their typing behavior may be correlated at a coarse-grained level even though they are not part of any attack. Our models allow for this type of behavior on the part of "normal" streams, and yet we will still be able to distinguish them from true steppingstone attacks.

Detection algorithms and give a hardness result when the attacker inserts "chaff" traffic in the stepping-stone streams. Our analysis shows that our detection algorithm is effective when the attacker inserts chaff that is less than a certain threshold fraction. Our hardness results indicate that when the attacker can insert chaff that is more than a certain threshold fraction, the attacker can make the attacking streams Mimic two independent random processes, and thus completely evade any detection algorithm.

Note that our hardness analysis will apply even when the monitor can actively manipulate the timing delay.

1. Initialize the local threshold parameter, C, □□and sampling interval□□t;
2. identify flows, f1. f2 …fn, and set count number of each flow to zero. $x_1 = x_2 = \ldots. = x_n = 0$;
3. when □T is over, calculate the probability distribution and the entropy variation as follows.

   Pi=xi (∑ x)

   $H(F) = -(p_i \log pi)$

   4. save x1, x2,...xn and H(F);

   5. if there is no dramatic change of the entropy variation H(F), namely, | H(F) – C | <□

Implementation:

- **Input**: Number of Node C=50 , Number of Packet Send□□□100, Time Interval t= 2 min
- **Step 1**:
  Flow Monitoring f (x1)
  First Iteration: C=10, Time t=20 [(10*2)], □□100
  For Example: C=8, t=16, □□□□□
  Pi= 8 * (8) = 64
- **Step 2**:
  Flow Monitoring f (x2)
  First Iteration: C=10, Time t=20 [(10*2)], □□100
  For Example: C=10, t=16, □□□□□□
  Pi= 64 * (10) = 640

Advantage:

- The local flow monitoring algorithm uses a entropy analysis.
- It uses upper stream for path determination monitoring from source to determination.

Disadvantage:

- In this algorithm, while sending a large amount of data, it send only a half of data but the other half of data cannot be sent properly. So again the half of data can be transmitted. The retransmission process can take more time to send the data.

B. ***QOD Routing Protocol***

First method, qualified neighbors chooses for packet forwarding by using QoS guaranteed neighbor selection method. Reduce the packet transmission time by using packet scheduling method. Resize the packets and assign smaller packets with mobility through packet resizing method. The traffic redundant elimination based transmission method used for increasing the transmission throughput. Finally soft deadline based forwarding method applying some packets are not feasible in packet forwarding to achieve the equality. In this proposed work QOD can achieve high mobility flexibility, scalability and disputation reduction.

Algorithm

- **Step 1**: if receive a packet forwarding request from a source node then
- **Step 2**: if this. SpaceUtility < threshold then Reply to the source node.
- **Step 3**: end if
- **Step 4**: end if
- **Step 5**: if receive forwarding request replies for neighbor nodes then
- **Step 6:** Determine the packet size Sp(i) to each neighbor I based on packet distribution.

S.no	SourceNode ID	Packet Size (Byte)	Performance Rate[%]	
			LFM	QOD-Routing
1	N1	1635	39.24	65.4
2	N2	593	35.58	71.16
3	N3	1365	39.00	74.45
4	N4	531	28.96	39.82
5	N5	658	30.36	48.90
6	N6	1677	34.70	43.74
7	N7	539	24.88	32.34
8	N8	1206	36.18	51.68
9	N9	1405	38.32	52.22
10	N10	649	32.45	55.62

Table 6.1 Performance Analysis of LFM and QOD-Routing Model

- **Step 7**: Estimate the queuing delay Tw for the packet for each neighbor based on location.
- Step 8: Determine the qualified neighbors that can satisfy the deadline requirements based on Tw and
- Sort the qualified nodes in descending order of Tw
- **Step 9**: Allocate workload rate Ai for each node based on node energy.
- **Step 10**: for each intermediate node ni in the sorted list do
- **Step 11**: Send packets to ni with transmission interval Sp(i)/ Ai.
- **Step 12**:end for

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

- **Step 13**: end if

Advantages

- The size of node information is small.
- The cluster head maintains most of the data.
- Path finding is efficient and routing performance is increased.
- Hierarchical routing does not need location information.
- Qualified neighbor nodes identification is easy even in worst case scenario (where number of nodes is very large).
- Implementation is made in real test bed.
- Unnecessary transmission is not occurred

6. EXPERIMENTAL ANALYSIS

The table contains sources ID, packet size and averages of performances rate details are shown. The comparison of Slice Based protocol performances rate is best for QOS-Distribute protocol.

This experimental result is analysis to QoS-guaranteed neighbor selection algorithm. The algorithm selects qualified neighbors and employs deadline-driven scheduling mechanism to guarantee QoS routing- Distributed packet scheduling algorithm. After qualified neighbors are identified, this algorithm schedules packet routing. It assigns earlier generated packets to forward with higher queuing delays, while assigns more recently generated packets to forward with lower queuing delays to reduce total transmission delay

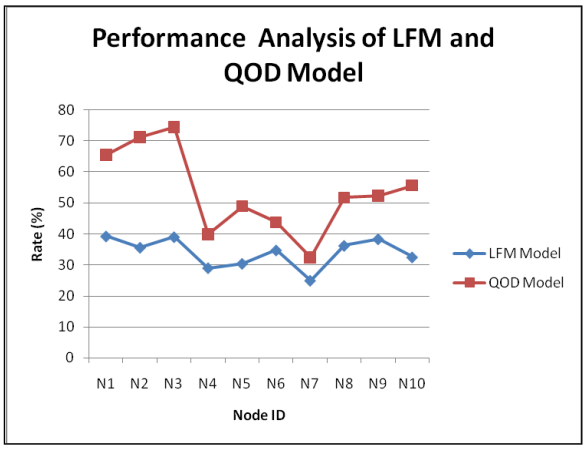

Fig 6.1 Performance Analysis of LFM and QOD-Routing Model

The figure 6.1 contains sources ID, packet size and averages of performances rate details are shown. The comparison of Slice Based protocol performances rate is best for QOS-Distribute protocol

7.CONCLUSION AND FUTURE ENHANCEMENT

The DDOS attack policy attribute-based encryption with user revocation scheme provides a big advantage by supporting user-defined time-specific authorization and fine-grained access control and data secure self-destruction. This survey paper proposes a cryptographic approach to enforce a fine-grained access control on the outsourced data that is dual encryption protocol exploiting the combined features of the encrypted text policy attribute-based encryption and group key management algorithm. The survey encryption scheme allows a data owner to define the access control policy and enforce it on multimedia content data to protect confidential data from unauthorized access in VANET.

In future, by improving the performance level of DDoS attack prevention has used in different algorithm will be applied in wireless network security and proposed schema will be tested against other type of attack.

REFERENCES

1. D. Boneh, X. Boyen, and E. Goh, “Hierarchical identity based encryption with constant size ciphertext,” in Proc. Annu. Int. Conf.Theory Appl. Cryptographic Techn., 2005, pp. 440–456.
2. C. Delerablee, P. Paillier, and D. Pointcheval, “Fully collusionsecure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys,” in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.
3. Z. Zhu, Z. Jiang, and R. Jiang, “The attack on mona: ecuremultiowner data sharing for dynamic groups in the cloud,” in Proc. Int.Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.
4. L. Zhou, V. Varadharajan, and M. Hitchens, “Achieving secure role-based access control on encrypted data in cloud storage,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
5. X. Zou, Y.-S. Dai, and E. Bertino, “A practical and flexible keymanagement mechanism for trusted collaborative computing,”inProc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.
6. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,“A view of cloud computing,” Commun. ACM, vol. 53, no. 4,pp. 50–58, Apr. 2010.
7. S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
8. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,“Plutus: Scalable secure file sharing on untrusted storage,”inProc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.
9. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing remote untrusted storage,” in Proc. etw. Distrib. Syst. SecuritySymp., 2003, pp. 131–145.
10. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improvedproxy re-encryption schemes with applications to secure distributed storage,” in Proc. Netw. Distrib. Syst. Security Symp., 2005,pp. 29–43.
11. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc.ACMSymp. Inf., Comput. Commun. Security, 2010, pp. 282–292.
12. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-basedencryption for fine-grained access control of encrypted data,”inProc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
13. R. Lu, X. Lin, X. Liang, and X. Shen, “Secure provenance: Theessential of bread and butter of data

forensics in cloudcomputing," in Proc. ACM Symp. Inf., Comput. Commun. Security,2010, pp. 282–292.

14. B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," in Proc. Int.Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
15. X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans.ParallelDistrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.