International Journal of Research
Available at
https://www.internationaljournalofresearch.org/
ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

Area of Research Is Privacy Protection Using Time and Attribute Based Control for Public Cloud

Kuruguntla Suman[1], Jalli Ajay [2]

[1]Assistant Professor,Department of Computer Science and Engineering Qis College of Engineering and Technology , Ongole, Prakasam Dist, Andhra Pradesh

[2]PG Scholar, Dept of CSE, QIS College of Engineering and Technology ,Ongole ,Prakasam Dist, Andhra Pradesh.

Abstract— an important problem in public clouds is how to selectively share documents based on fine-grained attribute-based access control policies (acps). An approach is to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and/or proxy re-encryption. However, such an approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires to keep multiple encrypted copies of the same documents; it incurs high computational costs. A direct application of a symmetric key cryptosystem, where users are grouped based on the policies they satisfy and unique keys are assigned to each group, also has similar weaknesses. We observe that, without utilizing public key cryptography and by allowing users to dynamically derive the symmetric keys at the time of decryption, one can address the above weaknesses. Based on this idea, we formalize a new key management scheme, called broadcast group key management (BGKM), and then give a secure construction of a BGKM scheme called ACV-BGKM. The idea is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. A key advantage of the BGKM scheme is that adding users/revoking users or updating acps can be performed efficiently by updating only some public information. Using our BGKM construct, we propose an efficient approach for fine-grained encryption-based access control for documents stored in an untrusted cloud file storage.

I. Introduction

Attribute based Mesh Networks (WMNs) are spreading to connect heterogeneous home users. Their aim is to support (mobile) users seamlessly with cheap and easy to maintain connectivity. The mesh topology of WMNs provides high flexibility as mesh routers are connected with multiple others providing the physical infrastructure for flexible routing and transport connections. Network virtualization can make use of this mesh topology by sharing, and also by combining links for desired network properties. Wi-Fi-based attribute based networks and mobile IP networks, WMNs have the advantages of low cost, easy deployment, self-organization and self-healing, and compatibility with existing wired and attribute based networks through the gateway/bridge function of mesh routers. A WMN consists of mesh routers and mesh clients [1]. Mesh routers are similar to ordinary routers in wired IP networks, except that they are connected via (possibly multichannel multi-radio) attribute based links. A major expected use of WMNs is as a attribute based backbone for providing

last-mile broadband Internet access [2] to mesh clients in a multi-hop way, through the gateway that is connected to the Internet. Because mesh clients may move within a WMN and change their points of attachment frequently, mobility management is a necessity for WMNs to function appropriately. Mobility management consists of location management and handoff management [3]. Location management keeps track of the location information of mesh clients, through location registration and location update operations. Handoff management maintains ongoing connections of mesh clients while they are moving around and changing their points of attachment. the different contextual features and preferences of the users in current WMN environments, the users need to be linked to different attribute based access networks with different bandwidth and robustness features, probably belonging to different Internet Service Providers (ISPs) with different security policies. The customers use different devices with different capabilities, which run different applications with different QoS requirements. As WMNs are edge networks connecting (mobile) users, they are expected to play an important role when introducing the required context-based user-centric networks. Moreover, WMNs are adaptable, self-configuring, and self-organizing to a high degree. As a consequence, WMNs are well suited to demonstrate the benefit of context-based approaches considering heterogeneous node capabilities and user preferences.

II. Two Phase Routing Based Schema

Routing-Based Schemes The iMesh [9] is an infrastructure-mode 802.11-based WMN. iMesh adopts a cross-layer approach for mobility management and develops a routing-based mobility management scheme. A link-layer handoff is triggered when a mesh client moves out of the covering area of its current serving mesh router. After the link-layer handoff is completed, the routing protocol used in iMesh, the Optimized Link State Routing (OLSR) protocol, broadcasts an HNA message announcing the new route of the mesh client. Mobility management in iMesh, therefore, incurs significant overhead due to the broadcasting of the HNA message. MEsh networks with MObility management (MEMO) [10] is the implementation of an applied WMN with support of mobility management. MEMO uses a modified AODV routing protocol, called as AODV-MEMO, for integrated routing and mobility management. Like the Ant scheme, MEMO also adopts MAC-layer triggered mobility management . Although this cross-layer design (Layers 2 and 3) helps reducing the handoff latency, the use of flooding by mesh clients to inform correspondence nodes about location handoffs leads to high signaling cost and bandwidth consumption. A common problem of iMesh and MEMO is that both of them are based on routing protocols proposed for mobile ad hoc networks that rely on broadcasting for route discovery or location change notification, thus excessive signaling overhead is incurred. WMM [5] is a novel-routing-based mobility management scheme proposed for WMNs. Location cache is used in combination with routing tables in the WMM scheme for integrated routing and location management. Because location update and location information synchronization can be done while mesh routers route packets, the WMM scheme does not incur significant signaling

overhead, as in tunneling-based and multicasting-based schemes. Additionally, as discussed in Section 7.3, the WMM scheme can be virtually viewed as a variant of mobility management schemes based on pointer forwarding, since relevant operations in the WMM scheme resemble forwarding pointer setup and reset operations in pointer forwarding approaches.

Algorithm 1. Two-Phase Validation - 2PV(TM).

1 Send "Prepare-to-Validate" to all participants
2 Wait for all replies (a True/False, and a set of policy versions for each unique policy)
3 Identify the largest version for all unique policies
4 If all participants utilize the largest version for each unique policy
5 If any responded False
6 ABORT
7 Otherwise
8 CONTINUE
9 Otherwise, for all participants with old versions of policies
10 Send "Update" with the largest version number of each policy
11 Goto 2

In the case of view consistency (Definition 2), there will be at most two rounds of the collection phase. A participant may only be asked to reevaluate a query using a newer policy by an Update message from the TM after one collection phase.

For the global consistency case (Definition 3), the TM retrieves the latest policy version from a master policies server (Step 2) and uses it to compare against the version numbers of each participant (Step 3). This master version may be retrieved only once or each time Step 3 is invoked. For the former case, collection may only be executed twice as in the case of view consistency. In the latter case, if the TM retrieves the latest version every round, global consistency may execute the collection many times. This is the case if the policy is updated during the round. While the number of rounds are theoretically infinite, in a practical setting, this should occur infrequently.4.2 Two-Phase Validate Commit Algorithm The 2PV protocol enforces trusted transactions, but does not enforce safe transactions because it does not validate any integrity constraints. Since the Two-Phase Commit atomic protocol commonly used to enforce integrity constraints has similar structure as 2PV, we propose integrating these protocols into a Two-Phase Validation Commit protocol. 2PVC can be used to ensure the data and policy consistency requirements of safe transactions. Specifically, 2PVC will evaluate the policies and authorizations within the first, voting phase. That is, when the TM sends out a Prepare-to-Commit message for a transaction, the participant server has three values to report

1) the YES or NO reply for the satisfaction of integrity constraints as in 2PC, 2) the TRUE or FALSE reply for the satisfaction of the proofs of authorizations as in 2PV, and

3) the version number of the policies used to build the proofs (vi; pi) as in 2PV. The process given in Algorithm 2 is for the TM under view consistency. It is similar to that of 2PV with the exception of handling the YES or NO reply for integrity constraint validation and having a decision of COMMIT rather than CONTINUE. The TM enforces the same behavior as 2PV in identifying policies inconsistencies and sending the Update messages. The same changes to 2PV can be made here to provide global consistency by consulting the master

policies server for the latest policy version (Step 5).

Algorithm 2. Two-Phase Validation Commit - 2PVC (TM).

1 Send "Prepare-to-Commit" to all participants
2 Wait for all replies (Yes/No, True/False, and a set of policy versions for each unique policy)
3 If any participant replied No for integrity check
4 ABORT
5 Identify the largest version for all unique policies
6 If all participants utilize the largest version for each unique policy
7 If any responded False
8 ABORT
9 Otherwise
10 COMMIT
11 Otherwise, for participants with old policies
12 Send "Update" with the largest version number of each policy
13 Wait for all replies
14 Goto 5

The resilience of 2PVC to system and communication
failures can be achieved in the same manner as 2PC by recording the progress of the protocol in the logs of the TM and participants. In the case of 2PVC, a participant must forcibly log the set of ðvi; piÞ tuples along with its vote and truth value. Similarly to 2PC, the cost of 2PVC can be measured in terms of log complexity (i.e., the number of times the protocol forcibly logs for recovery) and message
complexity (i.e., the number of messages sent). The logcomplexity of 2PVC is no different than basic 2PC and can be improved by using any of log-based optimizations of 2PCsuch as Presumed-Abort (PrA) and Presumed-Commit (PrC)

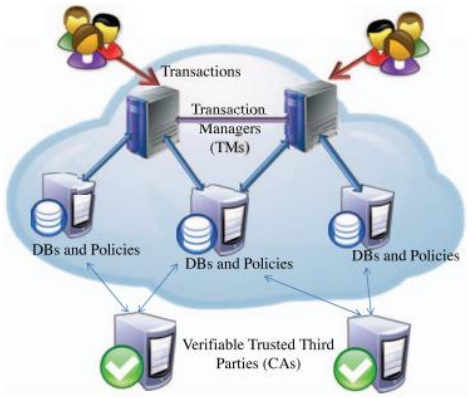
Attribute based mesh networks properties

The particular characteristics of WMNs [1] are derived from the (mesh) topology and the dynamics of attribute based environments. Instead of being another type of ad-hoc network, WMNs diversify the capabilities of ad-hoc networks, presenting low up-front costs, easy network maintenance, robustness, reliable service coverage, and minimal mobility of mesh routers. In addition to being widely accepted in the traditional application sectors of ad-hoc networks, WMNs are thus undergoing rapid commercialization in many other application scenarios, such as broadband home networking, community networking, building automation, and Internet access particularly in rural areas. At the same time, WMNs are already being used in free attribute based access initiatives, like funkfeuer1 and freifunk2 based on technology. Nevertheless, the distinct characteristics of WMNs, setting them apart from traditional attribute based networks, bring up new challenges to communication protocols, network management, reliability assurance, and security [1]. Scalability, for instance, has been identified as a major problem of important WMN protocols, but there are other open issues, such as the support of multicast applications and the utilization of multi-radios and multi-channels. In particular, the characteristics of the nodes have to be considered in the routing protocols since they can no longer be assumed to be similar. Proposed IP Forwarding Schemes the total

ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

communication cost as a function of K in both schemes, under different SMRs. The exists an optimal threshold K that results in minimized total communication cost. For example, when SMR1, the optimal K is 10 for the static anchor scheme, whereas it is 11 for the Two Phaseanchor scheme. Another observation is that the total communication cost in both schemes decreases, as SMR increases. This is because given fixed session arrival rates, the mobility rate decreases as SMR increases, thus the signaling cost incurred by location management as well as the total communication cost decreases. It is interesting to note in the Two Phaseanchor scheme always performs better than the static anchor scheme, under the given parameter values in Table 4 and the investigated SMRs. However, since, the Two Phaseanchor scheme incurs additional overhead of resetting the forwarding chain of an MC upon session arrival, it is expected that in cases that session arrival rates are considerably high, the additional overhead will offset its advantage. This is demonstrated, which plots the cost difference between the static anchor scheme and Two Phaseanchor scheme, as a function of SMR, when SMR is small, the Two Phaseanchor scheme performs better than the static anchor scheme. However, as SMR increases, there exists a crossover point beyond which the static anchor scheme starts performing better than the Two Phaseanchor scheme. It is interesting to see that there exists another crossover point of SMR beyond which the Two Phaseanchor scheme is superior again. This is because when SMR is considerably

III. Evolution Analysis



In this section a discussion is presented, which aims at giving first insights about important performance characteristics of the proposed solution for context-aware characterization and management of WMNs. To demonstrate the potential of proactive WMN management, we add prediction (mobility prediction) to the approach. we analyze the performance of the proposed schemes, in terms of the total communication cost incurred per time unit. Additionally, we compare the proposed schemes with two baseline schemes. In the first baseline scheme, IP forwarding is not used, meaning that every movement of an MC will trigger a location update event. Thus, it is essentially the same as having K in the proposed schemes. In the second baseline scheme, IP forwarding is employed, but the same threshold of the forwarding chain length is preset for all MCs, e.g., K for all MCs. We also carry out the performance comparison between our schemes and the WMM scheme proposed in [5]. A detailed description of the WMM scheme and the SPN model constructed for it will be given the parameters and their default values used in the performance evaluation. The time unit used is second. All costs presented below are normalized with respect to.

ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

IV. Conclusion

In this paper, the importance of introducing IP forwarding has been argued to provide highly adaptive WMNs. With the demand of such flexible WMNs, a novel architecture consisting of multiple virtual networks has been proposed and selected related work, which demonstrates the importance of providing solutions to integrate context in WMNs, has been surveyed. we plan to investigate how our proposed schemes can be extended to WMNs that have multiple gateways. In addition, we plan to investigate the proposed schemes under more realistic mobility models other than the random walk model. We will also investigate how caching of location information of MCs can be used to reduce the signaling cost incurred by our proposed schemes.

References:

1. Al-Oqily, I., & Karmouch, A. (2007). Policy-based context-aware overlay networks. In *Proceedings of information infrastructure symposium, GIIS*.
2. Al-Oqily, I., & Karmouch, A. (2007). Automating overlay networks management. In *Proceedings of 21st international conference on advanced networking and applications, AINA*.
3. Neto, A., Sargento, S., Logota, E., Antoniou, J.,&Pinto, F. (2009). Multiparty session and network resource control in the context casting (c-cast) project. In *Proceedings of 2nd international workshop on future multimedia networking, FMN*.
4. PlanetLab. *An open platform for developing, deploying, and accessing planetary-scale services*. Information available at http://www.planet-lab.org/.
5. VINI. *A virtual network infrastructure*. Information available at http://www.vini-veritas.net/.
6. GENI. *Global environment for network innovations*. Information available at http://www.geni.net/.
7. Feamster, N., Gao, L., & Rexford, J. (2007). How to lease the Internet in your spare time. *ACM SIGCOOM*, *37*(1), 61–64.
8. Subramanian, A., Buddhikot, M., & Miller, S. (2006). Interference aware routing in multi-radio attribute based mesh networks. In *Proceedings of 2nd workshop on attribute based mesh networks, WiMesh*.
9. Staub, T., Braun, T. (2008). Atom: adaptive transport over multipaths in attribute based mesh networks. In *Proceedings of 2nd ERCIM workshop on eMobility*.
10. Hu, P., Robinson, R., Portmann, M., & Indulska, J. (2008). Context-aware routing in attribute based mesh networks. In *Proceedings of CEASEMANS*.
11. I.F. Akyildiz, X. Wang, and W. Wang, "Attribute based Mesh Networks: A Survey," Computer Networks, vol. 47, no. 4, pp. 445-487, Mar.2005.
12. A. Raniwala and T.-c. Chiueh, "Architecture and Algorithms for an ieee 802.11-Based Multi-Channel Attribute based Mesh Network," Proc. IEEE INFOCOM, vol. 3, pp. 2223-2234, Mar. 2005.
13. I. Akyildiz, J. McNair, J. Ho, H. Uzunalioglu, and W. Wang, "Mobility Management in Next-Generation Attribute based Systems," Proc. IEEE, vol. 87, no. 8, pp. 1347-1384, Aug. 1999.
14. I. Akyildiz, J. Xie, and S. Mohanty, "A Survey of Mobility Management in Next-Generation All-IP-Based Attribute based

Systems," IEEE Attribute based Comm., vol. 11, no. 4, pp. 16-28, Aug. 2004.
15. D. Huang, P. Lin, and C. Gan, "Design and Performance Study for a Mobility Management Mechanism (WMM) Using Location Cache for Attribute based Mesh Networks," IEEE Trans. Mobile Computin vol. 7, no. 5, pp. 546-556, May 2008.
16. A. Boukerche and Z. Zhang, "A Hybrid-Routing Based Intra- Domain Mobility Management Scheme for Attribute based Mesh Networks," Proc. 11th Int'l Symp. Modeling, Analysis and Simulation of Attribute based and Mobile Systems (MSWiM '08), pp. 268-275, Oct. 2008.
17. H. Wang, Q. Huang, Y. Xia, Y. Wu, and Y. Yuan, "A Network- Based Local Mobility Management Scheme for Attribute based Mesh Networks," Proc. IEEE Attribute based Comm. and Networking Conf. (WCNC '07), pp. 3792-3797, Mar. 2007.
18. R. Huang, C. Zhang, and Y. Fang, "A Mobility Management Scheme for Attribute based Mesh Networks," Proc. 50th IEEE Global Telecomm. Conf., pp. 5092-5096, Nov. 2007.
19. V. Navda, A. Kashyap, and S. Das, "Design and Evaluation of iMesh: An Infrastructure-Mode Attribute based Mesh Network," Proc. Sixth IEEE Int'l Symp. World of Attribute based Mobile and Multimedia Networks (WoWMoM '05), pp. 164-170, June 2005.
20. M. Ren, C. Liu, H. Zhao, T. Zhao, and W. Yan, "MEMO: An Applied Attribute based Mesh Network with Client Support and Mobility Management," Proc. 50th IEEE Global Telecomm. Conf., pp. 5075-5079, Nov. 2007.

Author's Profile

K. SUMAN

* B. tech in S.V.H College of Engg and Tech, Machilipatnam
* M. Tech in Gokul Institute of Tech and Sciences, Vizianagaram
* Teaching Experience - 8Years
* Research Areas are Data Mining
* Present working as a Assistant Professor in QIS college of Engg and Tech, Ongole.

Jalli Ajay

* B. Tech(CSE) in QIS college of Engg and Tech, Ongole
* M. Tech(CSE) Scholar in QIS college of Engg and Tech, Ongole