International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 4, April 2014 ISSN 2319 - 4847

State-of-the-art of Privacy Preserving Data Aggregation Methods for MANET

Shanu Verma[1], S.V Pandit[2]

[1]Department of Computer Science & Engineering, ICOT, RGPV University, INDIA
[2]Assistant Professor, Department of Computer Science & Engineering, ICOT, RGPV University, INDIA

Abstract

Mobile Ad hoc NETworks (MANETs) have come out as a main future generation wireless networking technology. Mobile Ad Hoc Networks have been widely used in commercial and tactical domains. Privacy preservation is an important issue in today's context of extreme penetration of Internet and mobile technologies. It is more important in MANET environment because MANET accumulate sensitive or confidential data so privacy becomes an important concern. Providing efficient data aggregation while preserving data privacy is a challenging problem in MANET. MANET nodes are having resource limitation which includes power bottle neck too. To handle the issue of this limitation there are so many solutions which includes data aggregation technique too. MANETs face privacy breach risks and energy consumption.

Keywords: MANET, Privacy Preserving, *Data Aggregation, Power Efficient.*

1. INTRODUCTION

The Concept of mobile adhoc wireless devices working together in collaboration was given in earlier of 1990s. After that a significant amount of research has been carried on mobile adhoc networks (MANETs). Just because of devices' properties of mobility and scalability of wireless network, it is always in demand to use from very first day its' invention. Nowadays due to enhancing technology and reduced costs, MANETs have gained much more preferences over wired networks in the last couple of decades. Primary demands of MANETs are as follows: It should be robust, diverse, and re-silient computing environment and communication. MANET also required to enabling network-centric operation which could provide minimal down- time of network. At the other end, It is very obvious that MANET causes security risks because of its' nature and that is, mobile nodes are deployed in the open area. Almost all the application of the MANETs are in open area. The wireless communication makes the data/information accessible by anyone, who is trying to get it. Then he/she could intercept and manipulate the send data/information.

As we know that Mobile Ad hoc NETwork (MANET) is a group of all mobile devices which are equipped with both a wireless transmitter and a receiver. These wireless transmitters and receivers are responsible for communicate with each other nodes via bidirectional wireless links. There are two types of communication methods. These could be either direct or indirect.

Industrial remote access and control via wireless networks are becoming more and more popular these days [1]. One of the major advantages of wireless networks is its ability to allow data communication between different parties while maintaining their mobility too. All to gather we know that, the communication among these mobile nodes are dependent on the capacity of transmitters. This shows that two nodes can only communicate with each other only and only when they come into the range of each others' transmitter. MANET has its' solution too. In MANET communication could be done between those two nodes which are out of range by allowing third node which is an intermediate node by relay data transmissions. This concept of communication is further parted into two categories: first, single-hop and another is called multihop. In a single-hop network, only those nodes can communicate with each other which come within the transmitter range of each other. On the other end of table, in a multihop network, nodes can communicate with each other even though those are not belonging to each others' transmitter's range. Those can communicate with each other through another third node through rely concept. There are two variety of wireless network. Traditional wireless network would not have any fix or centralized infrastructure. As MANET would not require any fix centralized infrastructure; which gives empowered to all its' node to move freely and randomly [2], [3], [4]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, and this capability make MANET most suitable for many applications like military conflict, jungle fire, temporary application or emergency recovery. The main thing which is responsible for MANET demand is minimum configuration efforts and fast deployment where it is really very hard to find infrastructure to install. There are some scenarios for the same like disasters, military conflicts, and emergency situations [5], [6].

Because of various unique properties of MANET, it is becoming more popular and established in the industry [7], [8]. However, considering the fact that MANET is popular among various critical applications, security of network security plays a vital role. It is very unfortunate that because of open medium and various remote distribution of MANET make it vulnerable for different variety of attacks. At the other end, we can say because of lack of physical safety of nodes', various attackers can very easily hold and attack nodes to attacks. Most of the routing protocols related to MANETs

assume that each and every node in the MANET works with collaborations with each other nodes and most important it presumes that it is not malicious [9]. In this situation any attacker can easily crack security of MANETs by simply putting, malicious and non-collaborating nodes into the network.

2. PRIVACY PRESERVATION IN MANET ENVIRONMENT

Privacy preservation is playing an important issue while we discuss about any data repository in today's context of extreme penetration of network. This kind of privacy plays more vital role in the MANET where gathering of data is very frequent in network and in later part which could be very useful for processing and co-operative computations. This area researches preferred to apply various data mining techniques to preserve the privacy or secrecy of content. These techniques can also used in MANET nodes too.

There are number of techniques which are illustrated to effectively preserve the privacy of the source data. Randomization method is one of those very popular techniques. The randomization method is a technique in which noise is added to the data to be privacy-protected. This is done to mask the attribute values of records [10]. In this technique, a random noise value is added to the data which provides sufficiently large distance so that individual values cannot be recovered. After that, there are lot of techniques which are designed to get proper result from the perturbed data values. Subsequently, data mining techniques can be developed in order to work with these aggregate distributions. This randomization method has been part of traditional methods which are used in the area of perturbing data by any probability distribution method.

There are two major classes of privacy preservation schemes are applied. One is based on data perturbation techniques, in which some specific noise distribution is added to the data. Even after applying this distribution of the random perturbation, the desired result is achieved. In another technique, randomized data is used to data to mask the private values. However, data perturbation techniques have the drawback that they do not yield accurate aggregation results. It is noted by Kargupta et al. [11] that random matrices have predictable structures in the spectral domain. This predictability develops a random matrix-based spectral-filtering technique which retrieves original data from the dataset perturbing by removing or adding some random values. Perturbation is of two kinds. Additive Perturbation, in this a random noise is added to the private or personal data values. At the other end, Multiplicative Perturbation is there. In this perturbation random rotation techniques are used to get perturbed the values.

Secure Mult party Computation (SMC) and privacy preservation are related with each other with intimacy. Specially when we require to perform some process to hide the original data by third party. SMC problem was discussed by Yao [12] firstly, which gives a solution to Yao's Millionaire problem. SMC solution is meant for dealing with computing any function on any given input, in a distributed network in which each and every participant holds one input, which will be ensuring various things like input independence, rightness of the processing and computation, and certainly that will ensure that no information will get revealed to anyone in the computation [13].

3. DATA AGGREGATION IN PRIVACY PRESERVATION

Due to the energy limitation problem, in-network processing becomes an important area of research in MANET applications running at the application layer and scalability factor makes in-network processing very attractive. Data aggregation is part of in-network processing, which is called In-Network Aggregation (INA) [14]. In most of the in-network processing use cases security and privacy issues need to be taken care of with good amount of attention [13,15,16]. When the requirement is like that of Yao's millionaire problem [12], where the data cannot be revealed, concept like Tinysec [17] does not work. Tinysec has the serious flaw that data has to be encrypted and decrypted at aggregator node. There are numerous practical use cases where aggregated data result is important and the individual data values are to be kept private.

Consider the case of rating of television viewership, where the aggregated sum viewership result of a particular program is required by the surveying authority. But the advertisers or other third parties may be interested on the viewership details of the individual for their business interest. If any of participating party can be able to find micro details of particular or individual pattern of viewership, in that case, there is severe violation of privacy of the individual viewers. In another case, an authority is responsible for billing or for resource planning an individual's water consumption in monthly basis. In the case the authorization body gets the information on the daily water consumption pattern of the households some conclusion when the house is empty (when family members are gone out) can be disclosed. This can lead to theft attempt if that data is in some malicious hands. Apart from that there are innumerable applications, where data needs to be aggregated, but the content cannot be revealed.

4. PRIVACY PRESERVING AGGREGATION IN MANET: VARIOUS CATEGORIES

4.1 Power Efficient Techniques

4.1.1 PEPPDA (Power Efficient Privacy Preserving Data Aggregation)

Power efficient privacy preserving data aggregation method is very important in MANET because it concentrate on power preservation. In this existing protocol, it does not provide an power efficient solution for energy constrained and security required MANET. And this is just because of overhead of performing power consuming decryption and encryption at the

aggregator node for the data aggregation. Ultimately, this increased number of transmissions for achieving data privacy. Aggregator node will get increased the frequency of node compromise attack because of applying decrypting algorithm at it's end. That's the reason why aggregator node is responsible to reveal large amounts of data to adversaries. The privacy homomorphism based privacy preservation protocol achieves non delayed data aggregation by performing aggregation on encrypted data. It will decrease frequency of node compromise attack. So with this way sink will get accurate aggregated results with reduced communication and computation overhead. Where time and security play an important role this technique plays very importance and vial role. We have gone through all the above and come to now cited but when we think about its' various reason then we come to know that that are many reasons such as: privacy preservation, authenticity for data, data accuracy. Beside of these it also provides many other things as well like end to end confidentiality, energy efficiency and data freshness during data aggregation. This methods gives these all cited without overhead on the battery of sensors.

4.1.2 EEHA (Energy Efficient and High Accuracy secure Data Aggregation)

This [19] scheme is responsible to provides various quality aspects like high accuracy, secure data aggregation without releasing private sensor reading. This method provides all these without introducing considerable overhead on the battery limited sensors. It overcomes the issue of communication overhead by applying a slicing operation only at the leaf node.

4.1.3 Integrity-protecting Private Data Aggregation (iPDA)

This is another up gradation. iPDA [20] provides data privacy through slicing and assembling technique and at the other end it provides integrity through redundancy by constructing a disjoint aggregation tree.

4.1.4 ESPDA (Energy-Efficient Secure Pattern Based Data Aggregation)

This technique [21] is for improving the energy efficiency with the help of sending pattern code instead of original or actual data in Wireless Sensor Networks. End to end encryption key of each node is responsible for providing privacy. It also provides confidentiality and message authentication for the data.

4.2 Reduce Computational Effort Techniques

4.2.1 Slice-Mix-AggRegaTe (SMART)

The goal of this work is to bridge the gap between collaborative data collection by wireless sensor networks and data privacy. It [22] has the advantage of incurring less computation overhead. SMART is responsible for providing control on communication overhead, and accuracy of data aggregation.

4.2.2 Cluster-based Private Data Aggregation (CPDA)

This technique posses advantages in two folds, First, Clustering protocol, Second, Polynomials algebraic properties. It has the advantage of incurring less communication overhead [22]. Like any other cluster based concept, it also divided all nodes into different clusters. And in each cluster group, there is a cluster head which is responsible for further calculation and aggregation. Its main aim is to reduce computational efforts of node for processing and sending to the sink.

4.3 Privacy Preserving Data Mining Technique

4.3.1 Secure Multi-party Computation (SMC)

As it name shows that it deals with the problem of a joint computation of a function. Which will take input from multi-party's private data. Usually, It is uses public-key concept of cryptography technique. And this reason make this method very expensive in computations. This cost is very unsuitable for those resources which have power-constrains like MANET or wireless sensor networks [23, 24, 25].

4.3.2 Data Perturbation

This is another method of data mining to provide security to the original data. Under data perturbation method, a random number is chosen or taken from a some distribution. After choosing of that number method perform either addition/ multiplication to the data to make that converted. But still based on this perturbed data method can get the same results, while, maintaining the privacy achieved by using the randomized data to mask the private values. Another way around it has some drawbacks and that leads to inaccurate aggregation results. As shown by Kargupta et al. in [26] and by Huang et al. in [27], there are some data perturbation methods which cloud not preserve the privacy of the secrete personal data too.

4.4 Efficient Data Aggregation Technique

With many advantages of MANETs there are some disadvantages as well. MANET faces security risks and energy consumption issues. It is very challenging issue in any MANET to monitor cyber attacks and detection because of limited battery resources. To address this issue, method [28] has been developed which is of two types. First lossless and second, lossy aggregation techniques. This will reduce the energy cost in information transition and bandwidth consumption and at the same time it will preserving the expected detection accuracy. Moreover this paper proposes two methods for data under lossless aggregation techniques: First, compression based and second, event-based aggregation and at the other end, called lossy end, paper develops a lossy aggregation technique: feature-based aggregation. The main aim of these methods is to proposed such data aggregation techniques which will ultimately aggregate data in terms of the efficiency of energy consumption and detection accuracy.

5. PRIVACY PRESERVING AGGREGATION IN MANET: VARIOUS CATEGORIES

The mobile and dynamic nature of MANETs means that it is vital to protect them from modern sophisticated security attacks. In this paper we have presented a survey of significant privacy preserving, and we have reviewed privacy preserving and data aggregation methods that have been proposed in the literature.

Recently, Despites of many privacy preserving and data aggregation methods are become popular, the study of it is not just started. There have been many counter measures and related technologies to meet the challenge of privacy preserving data aggregation. This paper summarizes and analyzes some technologies of data aggregation to analysis the effect of privacy preserving in MANET environment, and gives some outlook for further study of the same with MAC authentication.

References

[1] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Trans. Instrum. Meas., vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

[2] G. Jayakumar and G. Gopinath, "Ad hocmobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[3] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[4] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[5] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[6] M. Zapata and N. Asokan, "Securing adhoc routing protocols," in Proc. ACM Workshop Wireless Secur., 2002, pp. 1–10.

[7] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile adhoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[8] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.

[9] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[10] R. Agrawal and R. Srikant, "Privacy-Preserving Data Mining," ACM Sigmod, pp. 439–450, 2000.

[11] H. Kargupta, S. Dutta, Q. Wang, and K. Sivakumar, "Random-data perturbation techniques and privacy-preserving data mining," Knowledge and Information Systems, vol. 7, no. 4, pp. 387–414, 2005.

[12] A. Yao, "Protocols for secure computations," 23rd Annual Symposium on Foundations of Computer Science, pp. 160–164, 1982.

[13] S. Goldwasser, "Multi-party computations: Past and present," 16th Annual ACM symposium on Principles of distributed computing, pp. 1–6, 1997.

[14] S. Peter, K. Piotrowski, and P. Langendoerfer, "On concealed data aggregation for WSNs," IEEE Consumer Communications and Networking Conference, pp. 192–196, 2007.

[15] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks," IEEE Infocom, pp. 2045–2053, 2007.

[16] J. Deng, R. Han, and S. Mishra, "Security Support for in network Processing in Wireless Sensor Networks," ACM Workshop on Security of Adhoc Networks, pp. 83–93, 2003.

[17] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," 2nd ACM Conference on Embedded Networked Sensor Systems, pp. 162–175, 2004.

[18] Joyce Jose, M .Princy, Josna Jose, "PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks," IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013), pp 330-336, 2013.

[19] Hongjuan Li, Kai Lin, Kequi Li, "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks", Computer Communication,34 (2011);591-597.

[20] W.He, X.Liu, H.Nguyen, K.Nahrstedt, T.Abdelzaher, "iPDA : An Integrity –Protecting Private Data Aggregation Scheme for Wireless Sensor Networks", IEEE MILCOM, November 2008, pp 1-7.

[21] Hassan Cam, Suat Ozdemir, Prashant Nair, Devasenapathy Muthuavinashiappan, H.Ozgur Sanli, "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands (ACM) 2006.

[22] He W,Liu X, Nguyen H, Nahrstedt K, Abdelzaher T, "PDA:Privacypreserving data aggregation in wireless sensor networks". Proceedings of 26th IEEE International Conference on Computer Communications (Infocom 2007), Anchorage, Alaska, USA, May 2007:2045-2053.

[23] A. C. Yao, "Protocols for secure computations," in 23rd IEEE Symposium on the Foundations of Computer Science (FOCS), 1982, pp. 160–164.

[24] I. D. Ronald Cramer and S. Dziembowski, "On the Complexity of Verifiable Secret Sharing and Multiparty Computation," in Proceedings of the thirty-second annual ACM symposium on Theory of computing, 2000, pp. 325–334.

[25] J. Halpern and V. Teague, "Rational Secret Sharing and Multiparty Computation," in Proceedings of the thirty-sixth annual ACM symposium on Theory of computing, 2004, pp. 623–632.

[26] H. Kargupta, Q. W. S. Datta, and K. Sivakumar, "On The Privacy Preserving Properties of Random Data Perturbation Techniques," in the IEEE International Conference on Data Mining, November 2003.

[27] Z. Huang, W. Du, and B. Chen, "Deriving Private Information from Randomized Data," in Proceedings of the ACM SIGMOD Conference, June 2005.

[28] Arijit Ukil, "Privacy Preserving Data Aggregation in Wireless Sensor Networks," 6th International Conference on Wireless and Mobile Communications IEEE-2010.