© 2015 IJSRSET | Volume 1 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Secure and Efficient Collaborative Load Balancing for Cluster-based MANETs

Kannan Sekar[1], Kannan VS[2], Kalaivani M[3]
Dhanalakshmi College of Engineering, Kancheepuram District, Tamilnadu, India

ABSTRACT

Mobile ad hoc networks (MANETs) are becoming increasingly common, and typical network loads considered for MANETs are increasing as applications evolve. Coordinated channel access protocols have been shown to be well suited for highly loaded MANETs under uniform load distributions. However, these protocols are in general not as well suited for non-uniform load distributions as uncoordinated channel access protocols due to the lack of on-demand dynamic channel allocation mechanisms that exist in infrastructure based coordinated protocols. In this paper, we present a lightweight dynamic channel allocation mechanism and a cooperative load balancing strategy that are applicable to cluster based MANETs to address this problem. We present protocols that utilize these mechanisms to improve performance in terms of throughput, energy consumption and inter-packet delay variation. A secure data transmission for cluster-based WSNs, where the clusters are formed dynamically and periodically. We propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks.

Keywords: Identity based digital signature, identity based online offline digital signature, hyper split module.

I. INTRODUCTION

Mobile ad hoc network have been an important class of network, providing communication support in mission critical scenarios including battlefield and tactical missions. This, in turn, increases the importance of bandwidth efficiency while maintaining tight requirements on energy consumption delay and jitter. Coordinated channel access protocols have been shown to be well suited for highly loaded MANETs under uniform load distributions. However, these protocols are in general not as well suited for non-uniform load distributions as uncoordinated channel access protocols due to the lack of on-demand dynamic channel allocation mechanisms that exist in infrastructure based coordinated protocols.

There are many dis-advantage in the existing scenario of load balancing concept some of the disadvantage are, Although sensor networks are being increasingly deployed in many application domains, assessing trustworthiness of reported data from distributed sensors has remained a challenging issue. Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system. In this context, assessing the trustworthiness of the collected data and announcing decision makers for the data trustworthiness becomes a challenging task.

As the computational power of very low power processors dramatically increases, mostly driven by demands of mobile computing

Such technology drops, WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms.
example is the recent emergence of multi-core and multi-processor systems in sensor nodes.

To overcome the existing concept we include some of the concepts they are, In this paper we propose two algorithms to cope with the non-uniform load distributions in MANETs: a light weight distributed dynamic channel allocation

Algorithm based on spectrum sensing, and a cooperative load balancing algorithm in which nodes select their channel access providers based on the availability of the resources. We apply these two algorithms for managing non uniform load distribution in MANETs into an energy efficient real-time coordinated MAC protocol, named MH-TRACE [4]. In MH-TRACE [4], the channel access is regulated by dynamically selected cluster heads (CHs). MH-TRACE [4] has been shown to have higher throughput and to be more energy efficient compared to CSMA type protocols. Although MH-TRACE incorporates spatial reuse, it does not provide any channel borrowing or load balancing mechanisms and thus does not provide Optimal support to non-uniform loads. Hence, we apply the dynamic channel allocation and cooperative load balancing algorithms to MH-TRACE, creating the new protocols of DCA-TRACE, CMH-TRACE and the combined CDCA-TRACE.

The advantages of the proposed system are as follows,

a) A light weight dynamic channel allocation scheme for cluster-based mobile ad hoc networks.
b) we propose a cooperative load balancing algorithm;
c) we incorporate these two algorithms into our earlier TRACE framework leading to DCA-TRACE and CMH-TRACE; and
d) We combine both algorithms to provide support for non-uniform load distributions and propose CDCA-TRACE.

II. NETWORK CONFIGURE

This module creates network structure such as server, client and some intermediate nodes. All Nodes are inter connected like wireless sensor network. A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

III. HYPER SPLIT

To fill the gap between theory and practice, in this paper, we propose a novel packet classification algorithm named Hyper Split. Compared to the well-known HiCuts and HSM algorithms, HyperSplit achieves superior performance in terms of classification speed, memory usage and preprocessing time. The practicability of the proposed algorithm is manifested by two facts in our test: HyperSplit is the only algorithm that can successfully handle all the rule sets.

After the hyper split process the packets are given with the generated random key. The keys are generated randomly using the scheme called SET_IBS. The scheme will generate key for each split packets it will give security for the packets.

IV. SECURE ANALYSIS

To send files from source to destination, files are converted to full secure format. Here we implement security to base on AES encryption algorithm and DSA algorithm. Key generation has two phases.

The first phase is choice of *algorithm parameters* which may be shared between different users of the system, while the second phase computes public and private keys for a single user. Each packet has a key to implement more security.

Here we use two schemes to make the security high, those are SET_IBS and SET_IBOOS.

The SET_IBS will generate random keys for the data's split by hyper split scheme. It will generate random keys for all the split data's so that if any hacker try to get the data's of any path, he will be need to provide the key obviously the hacker will not know the random key he will not able to get the data.

The SET_IBOOS is the another scheme which is also used here to make the security high. It is used to find out in which path or node the hacker hacks the data. So that where he tried to hack can also be known by us. So we can make the security high in that particular path.

V. REPUTATIONS OVER NETWORK

Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems - data aggregation and data trustworthiness assessment - using a single iterative procedure. Such trustworthiness estimate of each sensor is based on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is usually a weighted average sensors whose readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round of iteration their readings are given a lower weight.

VI. NODE AGGREGATION

Before the file reaches the destination node, grouping is done by combining all split data into one file using clustering methods. The receiver receives the file after decrypting the file using DSA key and displays the original files. Receiver also shows how many attackers have tried attack the file and checks the router names.

The DCA TRACE and CMH TRACE are used for the uniform load distribution, here the data's will be received to the receiver in non- uniform load distribution so these two schemes will not work here.

So we combine these two scheme and form a new trace for non-uniform load distribution it is CDCA TRACE. It supports the non-uniform load distribution. That is it will align the data's from various path in to the original data to decrypt.

VII. PERFORMANCE MESUREMENT

The performance measurement tracks the speed of file transfer, efficiency and generates report about node connectivity details. This allow us to check how many files has been transferred and in which nodes it has been transferred efficiently.

Here it is important to say about hyper split and SET_IBS scheme. The hyper split will split the data in to some parts, it will perform the process with high speed, and the process will get over in fraction of second.

Followed by the hyper split the SET_IBS scheme is used to generate the random keys for the split data. If we assign key for each split data it will more time. For smaller data it is possible but for larger data it is not possible, here SET_IBS scheme used to generate the random keys as faster as possible it will show the increase in performance. It saves time for assign the key by us.

The performance can be easily understand by the speed of it. For example the IBS assigning key for split data will be in fraction of second it will show the performance and CDCA search will concume the enery of router at low cost it increases the performance.

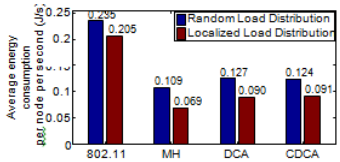

Fig. 1. Average energy consumption per node per seconds of the protocols.

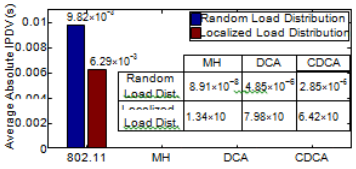

Fig. 2. Average absolute inter packet delay variation of the protocols.

VIII. LOAD BALANCING AND SECURITY SCHEME

The load balancing and the security schemes can be explained clearly with the system architecture given below

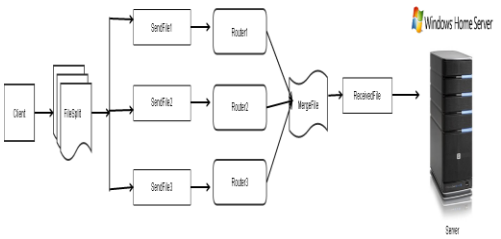

Figure 3 System Architecture

The above fig 3 is the architecture of our concept here, the data's to be sent from the source to destination will be encrypted with the encryption algorithm at the client end and the key generated will be sent to the receiver via email or any other mode.

The encrypted data will be split in to several packages in file split, and here SET_IBS scheme is used to generate key for every split packets. The several packets are allowed to pass through the cluster based scenario, that is many paths between the source and destination.

The several split packets are allowed to pass through all the three paths which reaches the destination. All the packets are grouped together in the mega file. The mega file will receive the packets in non-uniform. The CDCA TRACE is used to make it uniform and here the file will be decrypt with the random keys generated. Here the final data will be ready for further decryption in the receivers end.

After getting the data the receiver will decrypt the data with the key sent by the sender via email or some other source. After all these process the user can get the data's with high secutity. If any hackers hacks the data while it is coming in any of the three path in the diagram it will the exact location can be identified using the introduces scheme called IBOOS. The receiver can able to receive the data without any thought about the hackers its security level is high. It provides us high confidentiality.

IX. CONCLUSION

In this paper, we studied the problem of non-uniform load distribution in mobile ad hoc networks. We proposed a light weight dynamic channel allocation algorithm and a cooperative load balancing algorithm.The dynamic channel allocation works through carrier sensing and does not increase the overhead. It has been shown to be very effective in increasing the service levels as well as the throughput in the system with minimal effect on energy consumption and packet delay variation. The cooperative load balancing algorithm has less impact on the performance compared compared to the dynamic channel allocation algorithm. We showed that these two algorithms can be used simultaneously, maximizing the improvements in the system. We increased the security of the process. In case any hacker tried hacking the packets he cannot ablr to get the data. And we introduced a scheme called SET_IBOOS it show us where the hacker tried hacking and another scheme SET_IBS which generates random key for all splited packets it is very tough for the hackers to guess. So the security level of the process is increased.

X. REFERENCES

[1] B. Karaoglu, T. Numanoglu, and W. Heinzelman, "Analytical
[2] performance of soft clustering protocols," Ad Hoc Networks, vol. 9, no. 4, pp. 635–651, Jun. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2010.08.008
[3] IEEE 802.15.3 Working Group, "Part 15.3: Wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPAN)." IEEE Draft Standard, Draft P802.15.3/D16, Feb 2003.
[4] Institute of Electrical and Electronics Engineers, "IEEE Std 802.15.4-2006," Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), September 2006.
[5] B. Tavli and W. B. Heinzelman, "MH-TRACE: Multi hop time reservation using adaptive control for energy efficiency," IEEE Journal on Selected Areas of Communications, vol. 22, no. 5, pp. 942–953, June 2004.
[6] M. Kappes, "An experimental performance analysis of fMACg multicast in 802.11b networks for voip traffic," Computer Communications, vol. 29, no. 8, pp. 938 – 948, 2006, ¡ce:title¿Performance Evaluation of Wireless Networks and Communications¡/ce:title¿. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366405002161
[7] B. Leiner, D. Nielson, and F. Tobagi, "Issues in packet radio network design," Proceedings of the IEEE, vol. 75, no. 1, pp. 6 –20, jan. 1987.
[8] I. Cidon and M. Sidi, "Distributed assignment algorithms for multi-hop packet-radio networks," in INFOCOM '88. Networks: Evolution or Revolution, Proceedings. Seventh Annual Joint Conference of the IEEE Computer and Communcations Societies, IEEE, march 1988, pp. 1110 –1118.
[9] L. Gao and X. Wang, "A game approach for multi-channel allocation in multi-hop wireless networks," in Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing, ser. MobiHoc '08. New York, NY, USA: ACM, 2008, pp. 303–312. [Online]. Available: http://doi.acm.org/10.1145/1374618.1374659
[10] M. Felegyhazi, M. Cagalj, S. Bidokhti, and J.-P. Hubaux, "Noncooperative multi-radio channel allocation in wireless networks," in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, May 2007, pp. 1442 –1450.
[11] R. Ramaswami and K. Parhi, "Distributed scheduling of broadcasts in a radio network," in INFOCOM '89. Proceedings

of the Eighth Annual Joint Conference of the IEEE Computer and Communications Societies. Technology: Emerging or Converging, IEEE, april 1989, pp. 497 –504 vol.2.

[12] A. Ephremides and T. Truong, "Scheduling broadcasts in multihop radio networks," Communications, IEEE Transactions on, vol. 38, no. 4, pp. 456 –460, apr 1990.

[13] A. Sen and M. Huson, "A new model for scheduling packet radio networks," in INFOCOM '96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE, vol. 3, mar 1996, pp. 1116 –1124 vol.3.

[14] A. Raniwala and T. cker Chiueh, "Architecture and algorithms for an ieee 802.11-based multi-channel wireless mesh network," in INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 3, march 2005, pp. 2223 – 2234 vol. 3.

[15] L. Kleinrock and F. Tobagi, "Packet switching in radio channels: Part i–carrier sense multiple-access modes and their throughputdelay characteristics," Communications, IEEE Transactions on, vol. 23, no. 12, pp. 1400 – 1416, dec 1975.

[16] F. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part ii–the hidden terminal problem in carrier sense multipleaccess and the busy-tone solution," Communications, IEEE Transactions on, vol. 23, no. 12, pp. 1417 – 1433, dec 1975.

[17] P. Karn, "Maca-a new channel access method for packet radio," in ARRL/CRRL Amateur radio 9th computer networking conference, vol. 140, 1990, pp. 134–140.

[18] S. Toumpis and A. Goldsmith, "New media access protocols for wireless ad hoc networks based on cross-layer principles," Wireless Communications, IEEE Transactions on, vol. 5, no. 8, pp.2228 –2241, aug. 2006.

[19] D. Shukla, L. Chandran-Wadia, and S. Iyer, "Mitigating the exposed node problem in ieee 802.11 ad hoc networks," in Computer Communications and Networks, 2003. ICCCN 2003. Proceedings. The 12th International Conference on, oct. 2003, pp. 157 – 162.

[20] N. Jain, S. Das, and A. Nasipuri, "A multichannel csma mac protocol with receiver-based channel selection for multihop wireless networks," in Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on, 2001, pp. 432 –439.

[21] A. Nasipuri and S. Das, "Multichannel csma with signal powerbased channel selection for multihop wireless networks," in Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd, vol. 1, 2000, pp. 211 –218 vol.1.

[22] J. So and N. H. Vaidya, "Multi-channel mac for ad hoc networks: handling multi-channel hidden terminals using a single transceiver," in Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing, ser. MobiHoc '04. New York, NY, USA: ACM, 2004, pp. 222–233. [Online]. Available: http://doi.acm.org/10.1145/989459.989487

[23] K. Tang and M. Gerla, "Mac layer broadcast support in 802.11 wireless networks," in MILCOM 2000. 21st Century Military Communications Conference Proceedings, vol. 1, 2000, pp. 544–548 vol.1.

[24] J. Zhu and S. Roy, "Mac for dedicated short range communications in intelligent transport system," Communications Magazine, IEEE, vol. 41, no. 12, pp. 60–67, 2003.

[25] Institute of Electrical and Electronics Engineers, "IEEE Std 802.11-2007," Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.

[26] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks," in Proceedings of the 1st ACM 1536-1233 (c) 2013 IEEE.: DOI 10.1109/TMC.2014.2339215, IEEE Transactions on Mobile Computing 14 international workshop on Vehicular ad hoc networks, ser. VANET '04. New York, NY, USA: ACM, 2004, pp. 10–18. [Online]. Available: http://doi.acm.org/10.1145/1023875.1023878

[27] J. Xie, A. Das, S. Nandi, and A. Gupta, "Improving the reliability of ieee 802.11 broadcast scheme for multicasting in mobile ad hoc networks," in Wireless Communications and Networking Conference, 2005 IEEE, vol. 1, 2005, pp. 126–131 Vol. 1.

[28] X. Ma and X. Chen, "Performance analysis of ieee 802.11 broadcast scheme in ad hoc wireless lans," Vehicular Technology, IEEE Transactions on, vol. 57, no. 6, pp. 3757–3768, 2008.

[29] V. H. MacDonald, "Advanced mobile phone service: The cellular concept," Bell Syst. Tech. J., vol. 58, pp. 15–41, 1979.

[30] E. Standard, "Global system for mobile communications (gsm) standard for mobile phones," 1990.

[31] I. Katzela and M. Naghshineh, "Channel assignment schemesfor cellular mobile telecommunication systems: a comprehensive survey," Personal Communications, IEEE, vol. 3, no. 3, pp. 10 – 31, Jun. 1996.