A Survey of Achieving Efficient Channel Condition using Secure Channel Algorithm in Wireless Networks

M. Balaganesh
Associate Professor,
Dept of CSE
Sembodai Rukmani
Varatharajan Engineering
College
Sembodai, Tamilnadu

D. Balagowri
PG Scholar,
Dept of CSE
Sembodai Rukmani
Varatharajan Engineering
College,
Sembodai,Tamilnadu

P. Sathiya
PG Scholar,
Dept of CSE
Sembodai Rukmani
Varatharajan Engineering
College,
Sembodai,Tamilnadu

ABSTRACT

Wireless networking protocols square measure progressively being designed to use a user's measured channel condition. Every user reports its measured channel condition to a manager of wireless resources and a channel-aware protocol uses these reports to see however resources square measure allotted to users. In a channel-aware protocol, each individual user's reportable channel condition affects the performance of every alternative user. A doable attack against channel aware protocols is not an accurate feedback of channel condition. The preparation of channel-aware protocols will increase the risks exhibit by false feedback. In this paper, study the potential impact of associate offender that incorrectly reports its channel condition and propose a defense reaction to firmly estimate channel condition. Tend to analyze the mechanism and judge the system performance deploying the mechanism through simulation.

Keywords

Channel-aware, wireless communication

1. INTRODUCTION

Many protocols in fashionable wireless networks treat a link's channel condition information as a protocol input parameter; a tendency to decision such protocols channel-aware. Examples embrace timeserving schedulers, cooperative relaying network architectures, and economical unexpected network routing metrics. Even though every completely different application exploits the channel-condition info in different ways in which, the most goal of a channel-aware protocol is to boost system throughput by choosing a user or a path with sensible channel condition in a very given time instance. Most work on channel-aware protocols has principally targeted on however channel condition information is want to a lot of with efficiency utilize wireless resources. An implicit assumption of most past study is that every user properly reports channel condition information. However, this assumption will induce a security vulnerability since channel condition is uneven; specifically, because of potential channel condition imbalance, channel condition to a user will solely be measured and rumored by that user. Associate degree aggressor that misreports its measured channel condition may permit the aggressor to steal another users' service opportunities, for instance in a very setting wherever a centralized hardware schedules every user supported its channel condition. In another setting, a user chooses a next-hop forwarder supported the relayer's channel condition, during which case associate degree aggressor will misreport its channel condition to come up with a sink to lure packets to itself possibly for the aim of dropping those packets. In this paper, have a tendency to reveal the potential effects of false channel condition reportage in varied channel-aware network protocols and propose a defense that provides secure channel condition estimation. Our contributions are proposing a secure channel estimation formula which is used regularly applicable to any channel aware protocol. Tends to analyze the formula in terms of security and performance and analyze the result of misreported channel condition.

The false channel condition reportage attack that introduce during this paper is tough to spot by existing mechanisms, since our attack is generally protocol compliant; An offender have to be compelled to modify solely the channel-condition activity mechanism. Our attack will so be performed exploitation changed user instrumentation legitimately registered to a network. To the most effective of our information, the area unit the primary to check the false channel condition reportage attack in an exceedingly kind of network settings. Racic et al. take into account attacks supported false feedback to the PF hardware. In their work, as in our work, PF effectively resists false feedback; therefore their attack primarily works by exploiting the relinquishment method instead of the channel-aware nature of PF scheduler. They propose a secure relinquishment formula that\'s orthogonal to our approach of secure channel condition estimation.

Cellular network protocols have principally targeted on performance, ignoring security implications. To Illustrate, within the case of the programming formula, the base station fully trusts the reports from the UEs so as to realize its objective. Misreporting attackers benefit of this a prior trust so as to disrupt traditional network operations. Previous studies have principally targeted on one type of feedback; either inaccurate channel quality feedback or misreports of the packet transmission success. A tendency to take into account the impact of each feedback reports. a tendency to propose a variation of PF scheduler that creates use of quantification of traditional behavior to estimate and incorporate the reporting trust of each user.

2. RELATED WORKS

Padovani, R., Pankaj, R[5].: Data throughput of cdma-hdr a high efficiency data rate personal communication wireless system. Link is forward the data, throughput performance of a high data rate wireless access system is presented. The proposed system data is transmit to different access terminals in a TDM fashion by a forward link The rate transmitted to each access terminal is changeable and depends on each access terminal's measured SINR. Access Terminal send to the access points the index of the highest data rate which can be received reliably. The access point's scheduler determine the next terminal to be served based on the reported data rate requests from the terminals and the amount of data that has already been transmitted to each terminal. A cell layout of 19 3-sector and 6-sector hexagonal cells is considered. The forward link throughput of the embedded sector is simulated for stationary terminals. Delay in transmission and if the forwarder is not a trusted one, then the entire network may get damaged, it is one of the disadvantage. The advantage is transmission is reliable and able to find the next terminal based on the reported data.

Tse, D.N.C., Laroia, R.[14]: Opportunistic beam forming using dumb antennas. It is well proven that beam forming could significantly increase the performance of MIMO wireless system. The feedback and complexity associated with the beam forming schemes has hindered their use. On the other hand one can use multiuser diversity, which is a form of diversity inherent in a wireless network, provided by independent time-varying channels across the different users to achieve if not most some of the Benet associated with beam forming. The diversity Benet is exploited by tracking the channel actuations of the users and scheduling transmissions to users when their instantaneous channel quality is near the peak. The diversity gain increases with the dynamic range of the actuations and is thus limited in environments with little scattering and/or slow fading. In such environments, it has been proposed that the introduction of actuations at the transmitter could improve the overall schemes performance. Beam forming results to complexity and tracking the channel is difficult process is one of the main disadvantages. The advantage of this process is increases the overall performance and limited channel feedback.

E., Aazhang, B.[1]: Improving uplink capacity via user cooperation diversity. Mobile users' capacity is limited by the fact that within the duration of any given call, they experience severe variations in signal attenuation, thereby necessitating the use of some type of diversity. It are proposing a new form of diversity in this system. The diversity is necessary and variation in signal attenuation is one of the main demerit. It is more robust and user's achievable rates are susceptible which is the advantage of this scheme.

H. Luo, R. Ramjee, R., Sinha, P., Li, L.E., Lu, S[2].: Ucan: a unified cellular and adhoc network architecture. In third-generation wireless data networks, mobile users experiencing poor channel quality usually have low data-rate connections with the base-station. Providing service to low data-rate users is required for maintaining fairness, but at the cost of reducing the cell's aggregate throughput. In this paper, the Unified Cellular and Ad-Hoc Network architecture for enhancing cell throughput, while maintaining fairness. In Unified Cellular and Ad-Hoc Network, a mobile client has both third generation cellular link and IEEE 802.11-based peer-to-peer links. The third generation base station forwards packets for destination clients with poor channel quality to proxy clients with better channel quality. The proxy clients then use an ad-hoc network composed of other mobile clients and IEEE 802.11 wireless links to forward the packets to the appropriate destinations, thereby improving cell throughput. The third generation base station scheduling algorithm so that the throughput gains of active clients are distributed proportional to their average channel rate, thereby maintaining fairness. With the Unified Cellular and Ad-Hoc Network architecture in place, proposing novel greedy and on-demand protocols for proxy discovery and ad-hoc routing that explicitly leverage the existence of the third generation infrastructure to reduce complexity and improve reliability. Proposing a secure crediting mechanism to motivate users to participate in relaying packets for others. Through extensive simulations with HDR and IEEE 802.11b, the Unified Cellular and Ad-Hoc Network architecture can increase the individual user's throughput by up to 310% and the aggregate throughput of the HDR downlink by up to 60%. Poor channel quality and fewer throughputs is the main disadvantage. The advantage is increased throughputs and proposes a secure crediting mechanism in the scheme.

Tse and P. Viswanath[15].: A high-throughput path metric for multi-hop wireless routing [2, 3]**.** Presents the expected transmission count metric, which finds high-throughput paths on multi-hop wireless networks. Expected transmission count metric minimizes the expected total number of packet transmissions (including retransmissions) required to successfully deliver a packet to the ultimate destination. The Expected transmission count metric incorporates the effects of link loss ratios, asymmetry in the loss ratios between the two directions of each link, and interference among the successive links of a path. The minimum hop-count metric chooses arbitrarily among the different paths of the same minimum length, regardless of the often large differences in throughput among those paths, and ignoring the possibility that a longer path might offer higher throughput. This paper describes the design and implementation of Expected transmission count metric as a metric for the DSDV and DSR routing protocols, as well as modifications to DSDV and DSR which allow them to use Expected transmission count metric. Measurements taken from a 29-node 802.11b test-bed demonstrate the poor performance of minimum hop-count, illustrate the causes of that poor performance, and confirm that Expected transmission count metric improves performance. For long paths the throughput improvement is often a factor of two or more, suggesting that Expected transmission count metric will become more useful as networks grow larger and paths become longer. Poor performance of minimum hop count and poor performance is one of the disadvantages. The advantage is that improve throughput and minimizes the total number of packets.

Radmilo Racic, Denys Ma, Hao Chen, Xin Liu [12] Exploiting Opportunistic Scheduling in Cellular Data Networks. This paper presented the Third Generation cellular networks utilize time varying and location-dependent channel conditions to provide broadband services. They employ opportunistic scheduling to efficiently utilize spectrum under fairness constraints. Opportunistic scheduling algorithms rely on collaboration among all mobile users to achieve their design objectives. However, demonstrate that rogue cellular devices can exploit vulnerabilities in opportunistic scheduling algorithms, such as Proportional Fair (PF), to usurp the majority of time slots in third generation networks. opportunistic scheduling algorithms have been studied extensively [8, 9, 10].Our simulations show that only five rogue device per 50-user cell can use up to 90% of the time slots, and can cause 2 seconds of end-to-end inter-packet transmission delay on VoIP applications for every user in the same cell, rendering VoIP applications useless. To defend against these attacks, it explore several detection and prevention schemes, including modifications to the PF scheduler and a secure handoff procedure. Agarwal et al. [13] conducted a capacity analysis of shared control channels used for SMS delivery. They concluded that increasing volume and message sizescan significantly affect network performance. Enck etal. [14] presented a denial-of-service attack by sending a sufficient number of SMS messages per second to a range of cellular phones in the same area. An attacker would need only a single computer with a broadband network access to disrupt a network in a major city by saturating control channels shared between voice calls and SMSs. Traynor et al. evaluated this attack using a highly accurate GSM simulator and proposed mitigation strategies. warns that the paging channel is another scarce resource that an attacker on the Internet can overwhelm to cause a DoS attack. The disadvantage is that each jammer covers a very limited area and many traffic available in this system. The advantage is that it utilize the time varying and location-dependent channel condition to provide broadband services. The third generation network mainly used hand-off procedure and mainly focused on Dos attacks.

Soshant Bali1, Sridhar Machiraju2, Hui Zang2, and Victor Frost1[10]: Scheduler-Based Attacks in third generation Wireless Networks [10]. It produced a high-speed wide-area wireless networks have been rapidly proliferating; little is known about the strength and safety properties of these networks. In this paper, initial steps towards understanding these properties by studying Proportional Fair (PF), the scheduling algorithm used on the downlinks of these networks. and find that the fairness- ensuring mechanism of Proportional Fair can be easily corrupted by a malicious user to monopolize the wireless channel thereby starving other users. Using extensive experiments on commercial and laboratory-based CDMA networks, this vulnerability and quantify the resulting performance impact. find that delay jitter can be increased by up to 1 second and TCP throughput can be reduced by as much as 25− 30% by a single malicious user. Based on our results, argue for the need to use a more robust scheduling algorithm and outline one such algorithm. A small average achievable measurement rate and the performance is slow is one of the disadvantage. It is used various burst sizes and frequencies is one of the advantage.

Bogdan Carbunar, Ioannis Ioannidis, and Cristina Nita-Rotaru[18]: Hybrid networks consisting of cellular and Wi-Fi networks and it proposed as high-throughput architecture for cellular services. The networks, devices equipped with cellular and Wi-Fi network cards access Internet services through the cellular base station. The Wi-Fi interface is used to provide a better service to clients that are far away from the base station, via multihop, ad hoc paths. The modified trust model of hybrid networks generates a set of new security challenges as clients rely on intermediate nodes to participate effectively in the resource reservation process and data forwarding. JANUS [17,18], introduced a framework for scalable, secure and efficient routing for hybrid cellular and Wi-Fi networks. JANUS uses a scalable routing algorithm with multiple channel access, for improved network throughput. In addition, it provides protection against selfish nodes through a secure crediting protocol and protection against malicious nodes through secure route establishment and data forwarding mechanisms. The JANUS experimentally and show that its performance is 85% of the optimum algorithm, improving with a factor greater than 50% over previous work. the security overhead of JANUS against two type of attacks: less aggressive, but sufficient for some applications, selfish attacks, and purely malicious attacks. poor performance of minimum hop count and it effective only 85% is one of the disadvantage.

3. EXISTING SYSTEM

In existing system, the user reports the measured channel condition to the manager of the wireless resource. The channel-aware protocol uses these reports to see however resources are allotted to users. The false channel condition news attack is tough to spot by existing system, since the attack is generally protocol compliant. False channel condition is difficult to identify. Channel condition affects the performance of every other user. Suffers from invalid reservation and race condition problems.

4. CONCLUSION

The conclusion intended to study the various channel condition in wireless network. The data throughput of cdma-hdr a high efficiency data rate personal communication wireless system is used for how to sending the data in a efficient way. The opportunistic beam forming using dumb antennas is used for increasing the MIMO performance in wireless system. The improving uplink capacity via user cooperation diversity is used for measuring the capacity of uplink channels. Also it measures the quality of channel, improve the channel efficiency and control the data flow. The exploiting opportunistic scheduling in cellular data networks is used for determining the time vary in various generation such as third generation networks etc. The scheduler-based attacks in third generation wireless networks are used for measures the quality and performance of the downlink channels in a network. The hybrid networks consisting of cellular and Wi-Fi networks provides the high throughput in mobile networks. It is used to provide a better service to clients which are distance from the base station, via multi hop, ad hoc paths. For improving the network throughput in this system scalable routing algorithm with multiple channel access. The future work will be implemented to study the fault channel in wireless network. The false channel-feedback attack can arise in any channel aware protocol where a user reports its own channel condition.

5. REFERENCES

[1] E., Aazhang, B, "Improving uplink capacity via user cooperation diversity,"IEEE Trans. Mobile Computing, vol. 2, no. 2, pp. 161-173, Apr.-June 2003.

[2] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "Ucan: a unified cellular and ad-hoc network architecture," in Proceedings of the 9th annual international conference on Mobile computing and networking, pp. 353–367, ACM Press, 2003.

[3] J. Gomez, A.T. Campbell, M. Naghshineh, and C. Bisdikian, "PARO: Supporting Dynamic Power Controlled Routing in Wireless Ad Hoc Networks,"WirelessNetworks,vol. 9, no. 5, pp. 443-460, 2003.

[4] N. Agarwal, L. Chandran-Wadia, and V. Apte. Capacity analysis of the GSM short message service. In NationalConference on Communications, 2004.

[5] Padovani, R., Pankaj, R. (2000) 'Data throughput of cdma-hdr a high efficiency high data rate personal communication wireless system' pp. 353–36

[6] P. Mutaf and C. Castelluccia. Insecurity of the paging channel in the wireless internet: A denial-of-service attack that exploits dormant mobile IP hosts. In 3rd Workshop on Applications and Services in Wireless Networks, 2003.

[7] P. Viswanath, D. Tse, , and R. Laroia. Opportunistic Beamforming using Dumb Antennas. IEEE Transactions on Information Theory, 48:1277–1294, June 2002.

[8] R. Knopp and P. Humblet. Information capacity and power control in single-cell multiuser communications. In Proceedings of the ICC, 1995.

[9] R., Sinha, P., Li, L.E., Lu, S, "Ucan: a unified cellular and adhoc network architecture,"Proc. ACM MobiCom, pp. 134-146, 2003.

[10] S Soshant Bali1, Sridhar Machiraju2, Hui Zang2, and Victor Frost1. Scheduler-Based Attacks in third generation Wireless Networks. Technical Report RR06-ATL-040624, Sprint ATL, 2006.

[11] S. Singh and C. Raghavendra, "PAMAS—Power Aware MultiAccess Protocol with Signalling for Ad Hoc Networks,"ACM Computer Comm. Rev.,vol. 28, pp. 5-26, 1999.

[12] S. Singh, M. Woo, and C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," Proc. ACM MobiCom,Oct. 1998.

[13] Telecommunications Industry Association. CDMA 2000: High Rate Packet Data Air Interface Specification (TIA-856-A), 2004.

[14] Tse, D.N.C., Laroia, R "Opportunistic beam forming using dumb antennas,"IEEE Comm. Magazine,vol. 39, no. 6, pp. 138-147, June 2001.

[15] Tse and P. Viswanath. Fundamentals of Wireless Communication. Cambridge, 1 edition, 2005.

[16] W. Wei, C. Zhang, H. Zang, J. Kurose, and D. Towsley. Inference and Evaluation of Split-Connection Approaches in Cellular Data Networks. In Proc. of PAM, 2006.

[17] X. Li, H. Chen, Y. Shu, X. Chu, and Y.-W. Wu, "Energy Efficient Routing with Unreliable Links in Wireless Networks,"Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '06),pp. 160-169, 2006

[18] X. Liu, E. K. P. Chong, and N. B. Shroff. A framework for opportunistic scheduling in wireless networks. Computer Networks, 41(4):451–474, March 2003.

[19] X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and Energy-Efficient Routing for Static Wireless Ad Hoc Networks with Unreliable Links,"IEEE Trans. Parallel and Distributed Systems,vol. 20, no. 10, pp. 1408-1421,Oct.2009.