Detection of Exposed Terminal Problem in Wireless Networks – A Survey

Ms.Gomathi M[1] Dr.D.Prabakar[2] Dr. Karthik S[3]
[1]P.G. Student [2]Assiatant Professor [2]Dean
[1,2,3]Department of Computer Science Engineering
[1,2,3]SNS College of Technology, Coimbatore

Abstract— *The trust environmental bearer securing technique, used by wireless stations to gain access to the medium, is limited. In wireless networks, exposed terminal problem is common and leads to collision which constructs it complex to give the expected aspect of interactive domain services or support preference based services. To overcome these problems a directional antennas have been largely used in designing MAC protocols for wireless network. Directional receivers give various improvements over the universal receivers. In this paper, we represent that directional antennas can be exposed dynamically to clarify a normal disappear and uncovered terminal complication by using an energy efficient MAC protocol for wireless sensor networks. Exposed terminals are a main source in wireless networks that debases the network throughput act over highly revocation disturbance and threating concurrencies. To combat the exposed terminal trouble and used the sequence sharing in network. Here we compare and discuss some existing signature detection and various protocol techniques for eliminating terminal problems.*

Keywords— Signature Detection, Wireless Networks

I. INTRODUCTION

WN consists of spatially distributed sensor devices which monitor physical environment conditions, which employ a multi-hop data without a proper infrastructure due to their deployment nature. These networks are vulnerable to security threats, which includes minimum battery life, low processing power, small memory, deployment in hostile environment and the radio links are also insecure. An effective detection mechanism to prevent WN for a reliable transmission. Researchers often do not focus on security applications while designing a new routing protocol. Attacks are classified into internal and external. Eves dropping and inserting fault which causes Denial of Service (DoS) are external attacks. Internal attacks are motive by one of the nodes in sensor network. As there is no standard layered architecture of the communication protocol for wireless sensor network, each layer can be attacked due to their loophole nature. Routing attacks are vulnerable as they deal with Data Integrity. To protect from attacks, a security framework should be designed. Cryptographic techniques and certification are used to defend external attacks. The area of deployment is not physically protected and an attacker can easily process the node and capture some nodes. The software running nodes are tamper resistant and hence can be changed by a variety of internal attacks. Detection based techniques implemented so far can isolate attacker after recovers based techniques fail andInside attacks are not detected. Signature based approach also called specification based scheme and which is equal for WN in account of simple implementation and high detection rate. This paper proposes the signature based routing raids detection system, which secures wireless sensor networks from routing attacks. The aim of this work is to flow and implement the routing attacks for WNs. The proposed system includes three modules data gathering – which is used to collect data from neighbour nodes and filters the features; decision making-used to handle rules on the filtered data; attack detection- which compares the failure counter data with the threshold data. The attack is detected according to the above mentioned features.

II. THEORETICAL ANALYSIS

A. Medium Access Protocols

A best MAC protocols for the wireless sensor networks must be take care of the following attributes: the well-defined power efficient protocols in order to prolong the network lifetime. These sensor nodes are being a microelectronic device can only furnished with limited source of a power. The life time of sensor node is directory depending on batter life time. Other important attributes are measurability and adaptability to changes. Changes in node density, network size and topology should be handled rapidly and efficiently for a successful adaptation. Some of the reasons at the back of these are network's property mofications, limited node lifetime, and addition of new nodes to the network connectivity and since the network topology. A good quality of MAC protocol should gracefully contain such network changes.

B. Exposed Terminal Problem

In wireless networks, this complexity comes when a node is avoided from transmitting data to other nodes due to a nearby transmitter. Where the 2 receivers are out of sequence of each other, still now the more communications in the centre are in range of each other as represents in Figure 3. Here, if a transmission range user S1 and user R1 is keep place, user S2 is prevented from sending to node R2 as it concludes after carrier sense that it will interfere with the communication by its neighbour node S1. However note that node R2 could yet not get the dissemination of user S2 without collision since it is out of range from node S1.

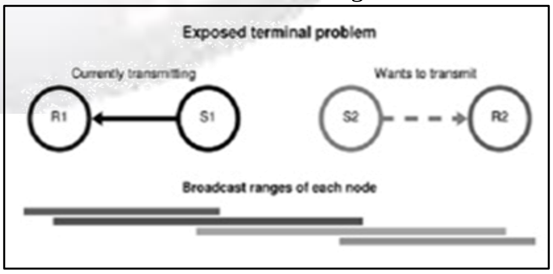

Fig. 1: Exposed Terminal Problem

IEEE 802.11 RTS/CTS mechanism helps to resolve this problem only if the nodes are synchronized. When a node hears an RTS from a neighbouring node, but not the equal CTS, that node can deduce that it is an exposed node and If the nodes are unsynchronized, the problem may occur that the sender will not heath CTS or the ACK during the communication of data of the second sender Fig.2.

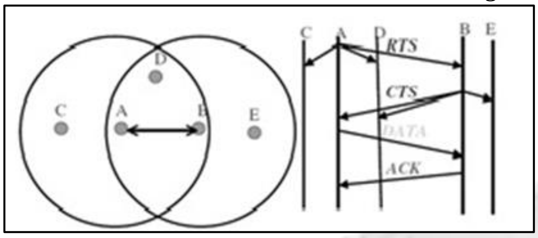

Fig. 2: RTS/CTS HANDSHAKE with ACK
RTS-CTS Handshake in process

- A is the source which is in the extent of B, D and C.
- B is the destination which is in the extent of A, D and E.
- A is the source which is in the extent of B, D and C.
- B is the destination which is in the extent of A, D and E.
- B sends ACK after getting one data packet.
- Improves link reliability using ACK Figure2

Multiple Access avoiding occurrence of Collision (MACA)

Information transfer duration is included in RTS and CTS, which helps in this time slot another node will be in patients.

If a RTS/CTS packet breakup's, nodes wait for an aimless time which is calculated using BEB algorithm

III. TECHNIQUES TO DETECTION OF EXPOSED TERMINAL PROBLEMS

Most of the Researchers have tried to come up with solutions to beaten the specified exposed problem with signature detection risk in WNs. Methods for both detection and prevention techniques to assist overcome this problem and the features of these models use for such purpose are discussed next.

A. Co-Map (Co-Occurrence Map) Approaches

CO-MAP (Co-Occurrence MAP) which advantages the location of devices to maintain exposed and hidden terminal problems in mobile WLANs so as to helps the multiple access efficiency. With the location data, CO-MAP rapidly builds a co-occurrence map showing which 2 connections can comes at the same time. Meanwhile, it selects the best settings of frame communications based on a novel technique domain method when hidden terminals are acclaimed.

B. Rigorous Mathematical Definitions

This paper is a first approach for an extensive and accurate article of EN and HN. There are three main contributions, described as follows: Providing rigorous definitions for EN and HN. Prepend studies of EN and HN have been based on incidental examples and the particular network range of nodes. Accurate explanation of EN and HN were missing. Without such rigorous definitions, it would be complex to devise extensive result to EN and HN and prove their validity under general details.

C. AC-MAC, a new MAC protocol

This paper presents a new MAC technology called C-MAC that is designed to achieve high-throughput bulk communication for info-intensive sensing uses. The key novelty of C-MAC is the exploitation of concurrent channel access based on empirical energy control and interference models. By increasing the system throughput, C-MAC also improves the energy efficiency of a network as nodes can be turned off for a longer period.

D. 802.11-based protocol without control messages

We design, implement, and evaluate 802.11ec (Encoded Control) as a prevents-message-free MAC. Alternative of authority information, 11ec works correlatable symbol sequences (CSSs) that, together with their transmission timing, convey all control data and change the fundamental design properties of the MAC. For example, 11ec replaces an 802.11 ACK message with a pretend ACK CSS that can be correlated instead of decoded.

E. A Cross Layer Design,

In summary, the main improvement of this paper over existing protocols in shared WLANs are as follows: We present a novel Attachment Coding scheme that enables nodes to communicate independent control messages on air, without degrading the performance of the original data communication on a full duplex paradigm. We represent a new Attachment Sense scheme that builds on top of the new coding technique, Attachment Coding, to solve both the hidden and exposed terminal attacks and increase the network throughput.

F. Attached-RTS MAC (AR-MAC)

To demonstrate the effectiveness of Attachment Coding, we propose a new cross-layer flow called Attached-RTS, which leverages exposed terminals for concurrent communications in distributed networks. Attached-RTS conducts of two parts: Attachment Coding in a PHY layer and closed-RTS MAC (AR-MAC) in an MAC layer. Attachment Coding attaches extraordinary designed RTS on info transmission, thus provides additional cue to authenticate current transmission.

G. IEEE 802.11 MAC Carrier sensing

As we have pointed out the RTS/CTS handshake of IEEE802.1 1 does not work well as we expected in theory. It cannot control hidden terminal problems completely. In this section, we explain this through a theoretical search. For good explanation, we first review the three radio ranges: (b) carrier sensing ratio represents the coverage within which a data is strongly collected if there is no occurrence from other radios.

H. IEEE 802.11 based ad hoc networks

In this paper, we represent that for the open space environment, the interference details of a receiver is 1.78 times the transmitter–receiver distance (under TWO-RAY GROUND path loss model). This implies that RTS/CTS handshake cannot function well when the transmitter–destination far is huge than 0.56 times the communication range. We then further analyse the efficient of RTS/CTS handshake behind like process and its connection with physical carrier monitoring.

I. Zigzag Decoding

In this paper, we propose an iterative Zigzag decoding algorithm to further improve the performance of multiple access communication. In the present technique, we exploit terms between the channel glossator and the Zigzag decoder. As the Zigzag decoder construct various types of soft assumptions of all data. These soft estimates are first decoded by channel decoder and the soft outcomes of shared funtionated designs from channel decoder are exploited to update the information in the received collided signal.

J. Symphony, A Packet Recovery Architecture

Although the idea behind Symphony is simple, here we having various complexities to know it in practical manner. In this paper, we use the methods proposed in Mozart for sender identification and RSS estimation. Find that decodethe collided packets. This leads to a different set of challenges as described.

K. Carrier sense multiple access with collision detection (CSMA/CD)

- Recognise a middle ground between CSMA/CD and CA.CSMA/CN is an early attempt to rethink medium access control protocols in wireless networks. This paper explores the first process in this direction, demonstrating that further progress is feasible and worth pursuing.
- Process the Collision Notification architecture with practical constraints in mind. We incorporate two methods ofself-signal controlling: 1) modelling and subtracting thewireless self-signal; and 2) sending the own-signal over aphysical wire, and then subtracting it with greater precision.

L. RTS/S-CTS mechanism, a novel symbol-level detection mechanism

In this paper, we address the above two problems as the remote hidden terminal problem due to the minimum SNR of the received CTS packet, and the CTS collision problem due to the low SINR of the received CTS packet. Both complications make the CTS packet un-decodable at hidden terminals under low SNR/SINR environments. Thus, it is a challenge to produce the desired NAV time information to those hidden terminals.

M. CSMA/CA-based, multi-hop, multi-rate wireless networks

We study the issue of balancing the interplay of spatial reuse (by tuning Tcs) and data rate selection (by selecting the highest possible info rate that can be uninterrupted for a given SINR value), with the ultimate objective of boosting the systems throughput. By extending Cali's model, we devise an analytical model that characterizes the communicating activities as governed by IEEE 802.11 DCF in a single-channel, multi-value, multi-hop wireless network, and getting the technique capacity as a function of Tcs, SINR, β, and other PHY/MAC systems parameters.

N. Symbol-level detection decoder (SLDD) and NAV decision algorithm

In this paper, we address the above two problems as the remote hidden terminal complication due to the low SNR of the received CTS packet, and the CTS collision problem due to the low SINR of the received CTS packet. Both complications make the CTS packet un-decodable at hidden terminals under low SNR/SINR environments. Thus, it is a challenge to obey the desired NAV time information to those hidden terminals. We reproduce a novel RTS/S-CTS mechanism that uses global known symbol sequences to carry the NAV time information.

O. SINR and Other PHY/MAC Systems Parameters

The rate of SINR act a major character in describes whether or not a communication is successful and/or the data rate the transmission sustain. In this paper, we study the issue of balancing the interplay of spatial reuse (by tuning Tcs) and packet ration chosen (by choosing the more positive packet ratio that can be continued for a given SINR value), with the extraordinary function of increasing the methods successive rate. By extending Cali's model, we describe a technique method that carries the communication processes as governed by IEEE 802.11 DCF in a single-channel, multi-value, multi-hop wireless network.

P. The Receiver-Based Auto Rate (RBAR) protocol

The novelty of RBAR is that its values adaptation techniques are in the destination alternative of in the source. This is in contrast to existing schemes in devices like the Wave- LAN II. We show that RBAR is better because it results in a more effective channel quality estimation which is then re directed in a higher overall throughput our protocol is based on the RTS/CTS mechanism and constant it can be integrated into various MAC protocols including the widely popular IEEE 802.11 protocol.

Q. Interference Cancellation &Zigbee Software Radios

In this paper, we explore whether it is possible to side step the performance adjustment among hidden and exposed terminals, by constructing receivers to recover multiple simultaneous levels. In this way, having complexity are low, permit exposed terminals to be more frequently tolerated as transmitters can choose a more aggressive sensing threshold.

R. Two-Sender Carrier Sense Based On Radio Propagation

This section presents a model of MAC throughput under different adequacy approach, analyze carrier impression to pure concurrency, pure multiplexing, and optimal selection between concurrency and complicated. The model requires the expected throughput ordinary over all possible validation of a network, given a set of parameters.

S. E-CSMA (Enhanced CSMA) protocols

Naive interpretation of carrier sense values, even when moderate over a window of time, can manage to unwanted interference and a misuse of empty channel bandwidth. Leveraging wireless channel assessment, implicit or explicit, from the received user to the transmitter, E-CSMA builds and maintains an analytically generated probability trading of packet reception success for each receiver, with respect to observable channel conditions at the transmitter. When a sender is meet with a broadcast/delay solution, these probability distributions are referred and indexed by current distributed channel.

T. The Performance of Ieee802.11 Dcf

We present to implement the information carried by the CTS packets transmitting/receiving node can evaluate the interference it generates on all the other growing transmissions, and conclude to transmit/receive if such interference does not corrupt the others. The basic ideas of our technique are comparable to the ones introduced in the Power Controlled Multiple Access (PCMA) proposed by Monks et al. Both protocols try to accomplish the capture event to increase the spatial reuse and, like PCMA, no station is allowed to transmit/receive if its transmission/ reception can destroy ongoing transmissions.

IV. CONCLUSION

In this paper, at first, we have explained the exposed terminal problem in wireless sensor networks. These problems have a collision on the performance of throughput. We have concisely interpreted the solution methods. After analysing the problems, we have discussed with multiple techniques like directional antenna based MAC protocol that used with MAC Protocol to increase the performance of the output of wireless sensor network. In this technique we can achieve better results, so that not well network appropriation and message of networks between each node can be avoided.

REFERENCES

[1] M. Vutukuru, K. Jamieson, and H. Balakrishnan, "Harnessing exposed terminals in wireless networks," in Proc. USENIX NSDI, 2008, pp. 59–72.

[2] L. B. Jiang and S. C. Liew, "Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks," IEEETrans. Mobile Comput. vol. 7, no. 1, pp. 34–49, Jan2008.

[3] M. Sha, G. Xing, G. Zhou, S. Liu, and X. Wang, "C-MAC: Model-driven concurrent medium access control for wireless sensor networks," in Proc. IEEE INFOCOM, 2009, pp. 1845–1853.

[4] E. Magistretti, O. Gurewitz, and E. W. Knightly, "802.11ec: Collision avoidance without control messages," in Proc. ACM MobiCom, 2012, pp. 65–76.

[5] L. Wang, K. Wu, and M. Hamdi, "Combating hidden and exposed terminal problems in wireless networks," IEEE Trans. Wireless Commun., vol. 11, no. 11, pp. 4204–4213, Nov. 2012.

[6] L. Wang and K. Wu, "Attached-RTS: Eliminating exposed terminal problem in wireless networks," IEEE Trans. Parallel Disturb. Syst., vol. 24, no. 7, pp. 1289 – 1299, Jul. 2012.

[7] IEEE Computer Society. 802.11n, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: Enhancements for higher throughput," 2009.

[8] K. Xu, M. Gerla, and S. Bae, "Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks," Elsevier Ad Hoc Networks, vol. 1, no. 1, pp. 107–123, Jul. 2003.

[9] S. Gollakota and D. Katabi, "Zigzag decoding: Combating hidden terminals in wireless networks," in Proc. ACM SIGCOMM, 2008, pp. 159–170.

[10] T. Bansal, B. Chen, P. Sinha, and K. Srinivasan, "Symphony: Cooperative packet recovery over the wired backbone in enterprise WLANs," in Proc. ACM MobiCom, 2013, pp. 351–362.

[11] S. Sen., R. R. Choudhury, and S. Nelakuditi, "CSMA/CN: Carrier sense multiple access with collision notification," in Proc. ACM MobiCom, 2010, pp. 25–36.

[12] T. Xiong, J. Zhang, J. Yao, and W. Lou, "Symbol-level detection: A new approach to silencing hidden terminals," in Proc. IEEE ICNP, 2012, pp. 1–10.

[13] X. Zhang and K. G. Shin, "E-MiLi: Energy-minimizing idle listening in wireless networks," in Proc. ACM MobiCom, 2011, pp. 205–216.

[14] T. Y. Lin and J. C. Houl, "Interplay of spatial reuse and SINR determined data rates in CSMA/CA-based, multi-hop, multi-rate wireless networks," in Proc. IEEE INFOCOM, 2007, pp. 803–811.

[15] G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive MAC protocol for multi-hop wireless networks," in Proc. ACM MobiCom, 2001, pp. 236–251.

[16] D. Halperin, T. Anderson, and D. Wetherall, "Taking the sting out of carrier sense: Interference cancellation for wireless LANs," in Proc. ACM MobiCom, 2008, pp. 339–350.

[17] M. Z. Brodsky and R. T. Morris, "In defence of wireless carrier sense," in Proc. ACM SIGCOMM, 2009, pp. 147–158.

[18] S. B. Eisenman and A. T. Campbell, "E-CSMA: Supporting enhanced CSMA performance in experimental sensor networks using per-neighbour transmission probability thresholds," in Proc. IEEE INFOCOM, 2007, pp. 1208–1216.

[19] M. Cesena, D. Maniezao, and M. Gerla, "Interference aware (IA) MAC: An enhancement to IEEE 802.11b DCF," in Proc. IEEE VTC, 2003, pp. 2799–2803.

[20] K. Mittal and E. Belding, "RTSS/CTSS: Mitigation of exposed terminals in static 802.11-based mesh networks," in Proc. IEEE WiMesh, 2006, pp. 3–12.