DETECTION OF NODE-MISBEHAVIOR USING OVERHEARING AND AUTONOMOUS AGENTS IN WIRELESS AD-HOC NETWORKS

Abstract

In Wireless Ad-hoc Networks, nodes co-operate among themselves to forward data packets from a source node to a destination node. Nodes may participate in route discovery or route maintenance process but refuse to forward packets due to presence of faulty hardware or software or to save their resources, such as, battery power and bandwidth. Detection and isolation of misbehavior nodes are important issues to improve the quality of communication service and to save resources of well behaving wireless nodes. In this work, firstly, a neighbor Overhearing based Misbehavior Detection(OMD) scheme is proposed. In OMD, each node overhears the transmissions of its neighbors and calculates packet forwarding ratio of its own as well as its neighbors. Source node uses the calculated information to identify a misbehaving node. Secondly, an Autonomous Agent based Misbehavior Detection(AAMD) technique is proposed. In AAMD, past behavior of nodes in the network is used as a metric to calculate the selection probability of a node. An agent residing at a node is activated using the activation key generated by a trusted third party to verify the misbehavior of the node. The proposed schemes reduce communication overheads and identification delays to detect misbehaving nodes in wireless ad-hoc network. Simulation results are presented to evaluate the performance of the proposed OMD and AAMD schemes.

A DISTRIBUTED FAULT-TOLERANT TOPOLOGY CONTROL ALGORITHM FOR HETEROGENEOUS WIRELESS SENSOR NETWORKS

ABSTRACT

In wireless sensor networks, the most common problem to deal with is energy efficiency, computational capacity and limited bandwidth. A new fault tolerant topology control algorithm is introduced to avoid the problems quoted above called “Disjoint Path Vector (DPV)”. The main objective of the proposed approach is to assign each sensor’s transmission range such that each has at least k-vertex-disjoint paths to super nodes and the total power consumption is minimum. The proposed algorithm guarantees the issues like casting problems and multihop transmissions by means of k-degree any cast Topology Control algorithm, which provides the transmission range such that each has at least k-vertex-disjoint paths to super nodes and the total power consumption is minimum. The resulting topologies are tolerant to node failures in the worst case. Along with DPV, we enhance the feature by means of adding Kautz-based REal-time, Fault-tolerant and EneRgy-efficient WSAN (REFER) to enhance the wireless sensor network fault tolerance level. REFER embeds Kautz graphs into the physical topology of a WSAN for real-time communication and connects the Kautz graphs using Distributed Hash Table (DHT) for high scalability. For all our proposed work guarantees the nature of energy efficiency and the fault tolerant level compare to all the algorithms proposed earlier.

ENERGETIC DATA COLLECTION USING MULTIPLE SINK MOBILITY IN WIRELESS SENSOR NETWORK

ABSTRACT

Mobile sink generation is the challenging task for wireless sensor networks (WSNs). In this system we propose to design an efficient routing protocol for single mobile sink and multiple mobile sink for data gathering in WSN. In this process, a biased random walk method is used to determine the next position of the sink. Then, a rendezvous point selection with splitting tree technique is used to find the optimal data transmission path. If the sink moves within the range of the rendezvous point, it receives the gathered data and if moved out, it selects a relay node from its neighbors to relay packets from rendezvous point to the sink. Proposed algorithm reduces the signal overhead and improves the triangular routing problem. In a wireless sensor network (WSN), how to conserve the limited power resources of sensors to extend the network lifetime of the WSN as long as possible while performing the sensing and sensed data reporting tasks, is the most critical issue in the network design. In a WSN, sensor nodes deliver sensed data back to the sink via multi-hopping. The sensor nodes near the sink will generally consume more battery power than others; consequently, these nodes will quickly drain out their battery energy and shorten the network lifetime of the WSN. Here the sink acts as a vehicle and collect the data from the sensor. The results show that the proposed model effectively supports sink mobility with low overhead and delay when compared with Intelligent Agent-based Routing protocol (lAR) and also increases the reliability and delivery ratio when the number of sources Increases. In this network transmissions a new kind of security traffic prediction is implemented with the help of RSA, once the communication begins ahead the transmitted data is encrypted and proceed. Once it reaches the destination node it automatically decrypts and collected in destination.

BRACER: A DISTRIBUTED BROADCAST PROTOCOL IN MULTI-HOP COGNITIVE RADIO AD HOC NETWORKS WITH COLLISION AVOIDANCE

Abstract

In wireless adhoc networking, broadcast is an essential medium, to control various routing operations via defined protocols. Spectrum availability is linear in the existing approaches, the problem here is broadcasting channels will be delivered via common medium and it is visible to all who are all available in network medium. Anyway the unlicensed users can also acquire different available channel sets in Cognitive Radio [CR] and Wireless Adhoc Networks. This non-uniform spectrum availability imposes special design challenges for broadcasting in CR ad hoc networks. In this proposed approach, a new protocol BRACER is introduced along with the base of classical protocol called AODV and DSR, which helps to prevent the collision in broadcasting network channels. In our proposed design, we consider practical scenarios that each unlicensed user is not assumed to be aware of the global network topology, the spectrum availability information of other users, and time synchronization information. By intelligently downsizing the original available channel set and designing the broadcasting sequences and scheduling schemes, our proposed broadcast protocol can provide very high successful broadcast ratio while achieving very short average broadcast delay. For all our proposed design proves our broadcast channels have full of efficiency to handle the network medium more innovative way and provides collision free network service in wireless medium.

Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks

Abstract

In wireless sensor network, two major challenges are lifetime enhancement and security problems. Once the security issues occurs in the wireless sensor network the entire lifetime will getting down with all its resources. A novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol is introduced, to manipulate the challenges caused in WSN such as security and lifetime. Energy Balance Control [EBC], a method which is used to accomplish the problem of network energy consumption, with the strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. A Probabilistic Random Walking method is introduced, in which it provides a quantitative security analysis on the proposed routing protocol. Our proposed approach experimentally proves that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. Once identifying and removing the non-uniform energy by means of secure routing schemes we can increase the lifetime and enhance the total number of messages delivery.

CONTROLLING AND PREVENTING MALICIOUS NODES VIA BAIT DETECTION SCHEME

ABSTRACT

In mobile impromptu networks (MANETs), a primary demand for the institution of communication among nodes is that nodes ought to get together with one another. Within the presence of malevolent nodes, this demand could cause serious security concerns; for example, such nodes could disrupt the routing method. During this context, preventing or detective work malicious nodes launching gray hole or cooperative black hole attacks may be a challenge. This paper makes an attempt to resolve this issue by coming up with a dynamic supply routing (DSR)-based routing mechanism, that is named because the cooperative bait detection theme (CBDS), that integrates the benefits of each proactive and reactive defense architectures. Our CBDS technique implements a reverse tracing technique to assist in achieving the expressed goal. Simulation results square measure provided, showing that within the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery quantitative relation and routing overhead.

Apart from the System we improve the network with additional paradigms like the source and destination data transferring mechanism is presented with some advanced security criteria. The source node defined the network pathway to destination by means of sending RREQ (Request) to next neighbor node, once the neighbor node provides RREP (Response), then only the path will be established between those two nodes and the next will be continuous as same manner. So, that there is no possibility of fake nodes enter into the channel and the malicious node attacks cannot happen into the system.

DESIGN AND PERFORMANCE ANALYSIS OF MOBILITY MANAGEMENT SCHEMES BASED ON POINTER FORWARDING FOR WIRELESS MESH NETWORKS

Abstract

We propose efficient mobility management schemes based on pointer forwarding for wireless mesh networks (WMNs) with the objective to reduce the overall network traffic incurred by mobility management and packet delivery. The proposed schemes are per-user-based, i.e., the optimal threshold of the forwarding chain length that minimizes the overall network traffic is dynamically determined for each individual mobile user, based on the user's specific mobility and service patterns. We develop analytical models based on stochastic Petri nets to evaluate the performance of the proposed schemes. We demonstrate that there exists an optimal threshold of the forwarding chain length, given a set of parameters characterizing the specific mobility and service patterns of a mobile user. We also demonstrate that our schemes yield significantly better performance than schemes that apply a static threshold to all mobile users. A comparative analysis shows that our pointer forwarding schemes outperform routing-based mobility management protocols for WMNs, especially for mobile Internet applications characterized by large traffic asymmetry for which the downlink packet arrival rate is much higher than the uplink packet arrival rate.

DETECTION OF BLACK HOLE ATTACKS IN MANETS BY USING PRINCIPLE OF EXCLUSION AND INCLUSION. (NEIGHBOR SET BASED METHOD)

ABSTRACT

There are many types of attacks in MANET. Generally speaking, these attacks can be classified into two broad categories: passive and active attacks. In passive attacks, the attackers typically involve eavesdropping of data, thus disclose the information of the location and move patterns of mobile nodes. This kind of attack is very difficult to detect, because the attacker seldom exhibits abnormal activities. Active attacks, on the other hand, involve actions performed by intruded. The target of the attack can be either data traffic or routing traffic. The intruders may insert large volume of extraneous data packets into networks. They can also intentionally dump, corrupt and delay data packets passing through it. In this paper, we are focusing on detecting black hole attack. One type of black hole attack can occur when the malicious node on the path directly attacks the data traffic by intentionally dropping, delaying or altering the data traffic passing through it. This type of black hole attack can be easily mitigated by setting the promiscuous mode of each node and listening to see if the next node on the path forward the data traffic as expected. Another type of black hole attack is to attack routing control traffic. The malicious node can impersonate some other node and advertise itself having the shortest path to the data source whose packets it is interested in. In this way, this malicious node becomes a black hole since the data traffic is misrouted to a wrong destination. We develop methods to detect this type of routing misbehavior caused black hole attack.

Efficient and Consistent Path loss Model for Mobile Network Simulation

Abstract:

In mobile network environment all the data transmissions purely depends on the quality of wireless channels. Each packet accuracy is dependent on the communication channels. Path loss is a major issue in every wireless mobile network scenario. The past approach path loss models are inaccurate, which requires excessive measurement or computational overhead, and/or often cannot be made to represent a given environment. The proposed framework contributes an adaptable way misfortune demonstrate that uses a novel methodology for spatially intelligible introduction from accessible adjacent channels to permit precise and effective demonstrating of way misfortune. We show that the proposed model, called Double Regression (DR), generates a correlated space, allowing both the sender and the receiver to move without abrupt change in path loss. Joining DR with a transient fading model, for example, Rayleigh fading gives a precise and effective channel demonstrate that we coordinate with the NS-2 simulator. In the proposed approach we utilize the estimations to accept the precision model for various situations as well as additionally demonstrate that there is significant effect on reproduction conduct when way misfortune is displayed precisely. Apart from the paper we improve the path consistency along with data security techniques such as AES and DES; we combine both these algorithms and form a proposed algorithm called Visual AES to make the data more secure while transmission.

A HIERARCHICAL KEY MANAGEMENT SCHEME FOR WIRELESS SENSOR NETWORKS BASED ON IDENTITY-BASED ENCRYPTION

ABSTRACT

Limited resources (such as energy, computing power, storage, and so on) make it impractical for wireless sensor networks (WSNs) to deploy traditional security schemes. In this paper, a hierarchical key management scheme is proposed on the basis of identity-based encryption (IBE).This proposed scheme not only converts the distributed flat architecture of the WSNs to a hierarchical architecture for better network management but also ensures the independence and security of the sub-networks. This paper firstly reviews the identity-based encryption, particularly, the Boneh-Franklin algorithm. Then a novel hierarchical key management scheme based on the basic Boneh-Franklin and Diffie-Hellman (DH) algorithms is proposed. At last, the security and efficiency of our scheme is discussed by comparing with other identity-based schemes for flat architecture of WSNs.

JOINT MOBILE DATA GATHERING AND ENERGY PROVISIONING IN WIRELESS RECHARGEABLE SENSOR NETWORKS

Abstract

The rising remote vitality exchange innovation empowers charging sensor batteries in a remote sensor system (WSN) and keeping up unending operation of the system. Late achievement here has opened up another measurement to the configuration of sensor system conventions. In the in the interim, versatile information gathering has been considered as a proficient distinct option for information handing-off in WSNs. Be that as it may, time variety of energizing rates in remote rechargeable sensor systems forces an incredible test in acquiring an ideal information gathering technique. In this system, we propose a structure of joint wireless energy replenishment and anchor-point based mobile data gathering (WerMDG) in WSNs by considering different wellsprings of vitality utilization and time-fluctuating nature of vitality recharging. To that end, we first decide the grapple point choice system and the succession to visit the stay focuses. We then plan the WerMDG issue into a system utility expansion issue which is obliged by stream, vitality equalization, connection and battery limit and the limited stay time of the versatile gatherer. Besides, we show a dispersed calculation made out of cross-layer information control, booking and steering subalgorithms for every sensor hub, and stay time allotment subalgorithm for the versatile authority at various grapple focuses. We likewise give the union investigation of these subalgorithms. At last, we actualize the WerMDG calculation in a conveyed way in the NS-2 test system and give broad numerical results to check the meeting of the proposed calculation and the effect of utility weight, join limit and reviving rate on system execution.

Joint Resource Allocation for Throughput Enhancement in Cognitive Radio Femtocell Networks

ABSTRACT

In psychological feature radio femtocell network (CRFN), secondary users (SUs) hand and glove sense a spectrum band to come to a decision the presence of primary network. However, this sensing overhead usually degrades the outturn performance. The previous work, to resolve this drawback, projected algorithms either to decrease the time spent in sensing or to decrease the quantity of mammal genus taking part in sensing. During this system, we have a tendency to propose a joint resource allocation (RA) strategy considering the time and energy consumed for spectrum sensing to maximize the outturn whereas satisfying the target detection performance in CRFN. Moreover, to cut back the resources employed in spectrum sensing to boot, we have a tendency to conjointly adopt the correct censored order statistics based mostly cooperative spectrum sensing theme that produces the criterion for deciding the set of coverage mammal genus. By therefore collectively coming up with the time and energy for sensing, the projected joint RA theme provides the development of spectral potency. Through simulation results, it's shown that the projected joint RA theme exhibits the improved performance over the standard ones in terms of total outturn of secondary networks. Apart from the Paper we make the additional things for forming separate FCs which can able to identify the node strength at the dynamic situations, once the node strength goes down, it provides the energy from Primary User, so that we can make a trustworthy environment. And the Primary User not directly involve into the transmissions, it carry over the complete responsibilities to the secondary user and the secondary user is responsible for transmission to the receiver, so that there is no possibility for intrusion and all.

Mobile Sink based Adaptive Immune Energy-Efficient Clustering Protocol for Improving the Lifetime and Stability Period of Wireless Sensor Networks

Abstract

In Wireless Sensor Network Energy Efficiency is a critical issue to handle with data transferring. Sensor Nodes located near by the sink nodes can grasp the energy quickly and acts smart to convey or transfer the data between one and another. This kind of energy grasping giving trouble to all the other nodes located far away from the sink nodes. Misusing the portability of a sink has been generally acknowledged as a proficient way to lighten this issue. In any case, deciding an ideal moving direction for a portable sink is a NP-Hard issue. So that a new protocol design is implemented called Mobile Sink based adaptive Immune Energy-Efficient clustering Protocol (MSIEEP) to eliminate the energy consuming holes and prove the system to be more efficient and stable compare to the existing systems. MSIEEP uses the Adaptive Immune Algorithm (AIA) to guide the mobile sink based on minimizing the total dissipated energy in communication and overhead control packets. AIA is used to identify the generalized number of Cluster Heads [CHs], to enhance the lifetime and stability period of the network. The performance of the proposed approach to be compared with the existing protocols like LEACH, LEACHGA, A-LEACH, rendezvous and MIEEPB using NS2 simulation environment and prove the proposed approach is tolerant and energy efficient compare to the works defined already. Apart from this the proposed approach proves the mobile sink increases the ability of the proposed protocol to deliver packets to the destination.

MODELING AND ANALYSIS OF LEAP, A KEY MANAGEMENT PROTOCOL FOR WIRELESS SENSOR NETWORKS

ABSTRACT

A formal investigation of a key administration rule, called LEAP (Localized Encryption and Authentication Protocol), expected for wireless network systems is displayed in this proposed work. LEAP is modeled by utilizing the abnormal state formal dialect HLSPL furthermore, checked utilizing the NS2 infrastructure for attacks on the security as well as credibility of the data transmission between source and destinations. We concentrate on the proposed protocol foundation of pair wise keys for closest neighbors and for multi hop neighbors. We then utilize this establishment to test the protocol technique for group key redistribution. At long last, we check utilization of LEAP with μTESLA, a confirmation protocol used a one way key chain and deferred key exposure, which LEAP employments for validation of node denial messages. For all our results will prove the analysis of proposed architecture and shows that it has the ability to work under proper authentication and data privacy mechanisms.

Advanced Multi-Path Routing Methodology with Energy Efficient MANET Based Traffic Splitting Technique

ABSTRACT:

MANETs have an advantage to choose the path dynamically and move the packets with limited amount of bandwidth and limited power consumption of nodes. Due to these advantages it affects in some complex network scenarios such as, when multiple source nodes connecting with destination it is unstable and go down at any time, making communication over mobile ad hoc networks difficult. A new methodology is required to solve these issues over MANET, so that a new mechanism called "Traffic Aware Routing Identification" is established to provide the transmission capacity of MANET more perfect as well we this scenario works fine for all cases like single path and multi-path terminologies. This methodology clearly checks the neighbor nodes bandwidth, delay and path stability before going to start transmitting data to the destination via that defined path. If the path does not satisfy the routing constraints, then the traffic can be distributed along the multiple disjoint paths, using the Traffic Splitting algorithm. For the entire network scenario clearly illustrates the trustworthy and successful transmission of with reduced delay between source and destination. Along with this we improve the security mechanism to data transmission by means of adding the crypto constraints to the transmitting data, so no one can interrupt and misusing the data without the knowledge of source and destination.

NEIGHBOR SIMILARITY TRUST AGAINST SYBIL ATTACK IN P2P E-COMMERCE

Abstract

Peer to Peer (P2P) e-commerce applications exist at the edge of the Internet with vulnerabilities to passive and active attacks. These attacks have pushed away potential business firms and individuals whose aim is to get the best benefit in ecommerce with minimal losses. The attacks occur during interactions between the trading peers as a transaction takes place. In this paper, we propose how to address Sybil attack, an active attack, in which peers can have bogus and multiple identities to fake their owns. Most existing work, which concentrates on social networks and trusted certification, has not been able to prevent Sybil attack peers from doing transactions. Our work exploits the neighbor similarity trust relationship to address Sybil attack. In our approach, duplicated Sybil attack peers can be identified as the neighbor peers become acquainted and hence more trusted to each other. Security and performance analysis shows that Sybil attack can be minimized by our proposed neighbor similarity trust.

PERFORMANCE ANALYSIS OF AODV AND WCETT ROUTING PROTOCOLS IN COGNITIVE RADIO AD-HOC NETWORK (CRAHN)

ABSTRACT

In the past few years, cognitive radio paradigm has emerged as a solution to avoid problems of spectrum scarcity and inefficiency in spectrum usage. Cognitive Radio (CR) capable to identify the unused spectrum in order to allow CR users to occupy it without interfering the primary users (PUs). Routing is a crucial task in CR network (CRN) due to diversity in available channels. In this paper, Ad-Hoc On-Demand Distance Vector (AODV) and Weight Cumulative Expected Transmission Time (WCETT) routing protocols used to address the efficient route selection between the source and destination in a Cognitive Radio Ad-Hoc Network (CRAHN). The performance of AODV and WCETT is evaluated on the basis of average throughput in three kinds of routing structure to satisfy different requirements from users: 1) single radio multi-channels, 2) equal number of radios and channels and 3) multi-radios multi-channels. The simulation result shows AODV has a significant average throughput in single radio multi-channels where the average throughput is 48.25% higher compared to average throughput in WCETT. However, WCETT has a significant average throughput in equal number of radios and channels; as well as in multi-radios multi-channels where the difference of average throughput is 38.22% and 34.63% respectively.

RANGE-FREE LOCALIZATION APPROACH FOR M2M COMMUNICATION SYSTEM USING MOBILE ANCHOR NODES

Abstract

Most existing range-free localization approaches use static anchor nodes. These approaches cannot be used for large scale Machine to Machine (M2M) communication networks since a fixed number of static anchor nodes cannot localize Machine Type Communication (MTC) devices such as sensors whenever more MTC devices are deployed in the network. Thus, this article introduces a Range-free, Energy efficient, Localization technique that uses Mobile Anchor (RELMA) nodes. This approach is scalable since the anchor nodes can move close to the newly deployed MTC devices in the network to localize them. The un-localized MTC devices receive beacon messages with the location information of mobile anchors whenever the anchors are within the sensing range of un-localized devices. Thus, RELMA is energy efficient and accurate because (i) the sensing range is much shorter than the communication range that other approaches use, and (ii) the intersected region of three sensing circles, where the un-localized device resides in, is very small. Simulation results show that RELMA outperforms existing Neighbor information Based Localization Scheme (NBLS) and Sink at the Origin Localization (SOL) approaches in terms of localization error and network energy consumption.

SECRECY CAPACITY OPTIMIZATION VIA COOPERATIVE RELAYING AND JAMMING FOR WANETS

ABSTRACT

In the WANET environment, the most satisfiable network communications are carried out via cooperative networks. The cooperative network relaying architecture system can provide better operational efficiency and reliability by acquiring more accurate and timely information, which automatically leads Qos in transmissions. In case of security concerns, the cooperative network has to improve their ability to provide support to the nodes present into the network region. In this approach, we introduced physical layer security to provide secure cooperative communication for wireless ad hoc networks (WANETs) where involve multiple source destination pairs and malicious eavesdroppers. By describing the security execution of the framework by secrecy limit, we think about the secrecy limit streamlining issue in which security improvement is accomplished by means of helpful handing-off and agreeable sticking. In particular, we propose a framework model where an arrangement of hand-off nodes can be misused by various source destination sets to accomplish physical layer security. We hypothetically exhibit a comparing plan for the transfer task issue and build up an ideal calculation to tackle it in polynomial time. To further build the framework mystery limit, we abuse the agreeable sticking method also; propose a savvy sticking calculation to meddle the listening in channels. Through broad investigations, we accept that our proposed calculations fundamentally expand the framework mystery limit under different system settings.

Secure Intrusion Detection System for Authentication in Wireless Sensor Networks

Abstract:

Wireless Sensor Network is an indivisible part of network where it has no infrastructure. In the past, Intrusion detection systems were used to detect intrusions in network effectively. Most of the systems are able to detect intrusions with high false alarm rate. In this paper, we propose a Fuzzy based Secure Intrusion Detection System (FSIDS) for detecting malicious activities and providing authentication as well as data integrity. To achieve this, Cluster based routing is established based on trust vector of neighbor nodes in random topology. Certificate based trust recommendation is estimated based on packet identification, certification revocation record and packet receiving capability for identifying and isolating the malicious nodes in network. Simulation results shows that the FSIDS provides better detection efficiency, packet delivery ratio, low end to end delay, successful certification rate and low overhead than existing schemes.

SOFTWARE DEFINED GREEN DATA CENTER NETWORK WITH EXCLUSIVE ROUTING

Abstract

The explosive expansion of data center sizes aggravates the power consumption and carbon footprint, which has restricted the sustainable growth of cloud services and seriously troubled data center operators. In recent years, plenty of advanced data center network architectures have been proposed. They usually employ richly-connected topologies and multi-path routing to provide high network capacity. Unfortunately, they also undergo inefficient network energy usage during the traffic valley time. To address the problem, many energy-aware flow scheduling algorithms are proposed recently, primarily considering how to aggregate traffic by flexibly choosing the routing paths, with flows fairly sharing the link bandwidths.

In this paper, we leverage software defined network (SDN) technique and explore a new solution to energy-aware flow scheduling, i.e., scheduling flows in the time dimension and using exclusive routing (EXR) for each flow, i.e., a flow always exclusively utilizes the links of its routing path. The key insight is that exclusive occupation of link resources usually results in higher link utilization in high-radix data center networks, since each flow does not need to compete for the link bandwidths with others. When scheduling the flows, EXR leaves flexibility to operators to define the priorities of flows, e.g., based on flow size, flow deadline, etc. Extensive simulations and testbed experiments both show that EXR can effectively save network energy compared with the regular fair-sharing routing (FSR), and significantly reduce the average flow completion time.

VEHICULAR AD-HOC NETWORKS (VANETS) DYNAMIC PERFORMANCE ESTIMATION ROUTING MODEL FOR CITY SCENARIOS

ABSTRACT:

Vehicular Ad-hoc Networks (VANET) is one of the most actual and challenging research area in automotive companies and ITS designers. In general, a VANET is formed from a number of vehicles which are in the same road to form ad-hoc network. The presence of such these networks opens the way for a wide range of applications such as safety applications, mobility and connectivity for both driver and passengers to exploit the transport systems in a smoothly, efficiently and safer way. For safety applications which is a critical section from VANET, the best routing protocol must be selected. Indeed, it is important and essential to test and evaluate different routing protocols that related to VANET system before apply them in the real environment which can be done via VANET simulation tools. This paper evaluates the performance of three different routing protocols for VANET system in city of Khartoum. The performance are evaluated and compared in terms of PDR, average throughput, delay and total energy. Our objective is to estimate the performance of routing model for city scenario. The main goal is to find the suitable routing protocol in a high density traffic area in Khartoum. We have considered three routing protocols DSR, AODV and DSDV. The results indicate the bad performance of DSDV protocol which is a type from proactive routing protocols. The AODV protocol achieves maximum average throughput which is equals to 330.07Kbps. The minimum value of delay is obtained from using DSR protocol was 15.81 ms.

WORMHOLE ATTACK DETECTION ALGORITHMS IN WIRELESS NETWORK CODING SYSTEMS

ABSTRACT:

Network coding has been shown to be an effective approach to improve the wireless system performance. However, many security issues impede its wide deployment in practice. Besides the well-studied pollution attacks, there is another severe threat, that of wormhole attacks, which undermines the performance gain of network coding. Since the underlying characteristics of network coding systems are distinctly different from traditional wireless networks, the impact of wormhole attacks and countermeasures are generally unknown. In this paper, we quantify wormholes' devastating harmful impact on network coding system performance through experiments. We first propose a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, we proposes DAWN, Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the change of the flow directions of the innovative packets caused by wormholes. We rigorously prove that DAWN guarantees a good lower bound of successful detection rate. We perform analysis on the resistance of DAWN against collusion attacks. We find that the robustness depends on the node density in the network, and prove a necessary condition to achieve collusion-resistance. DAWN does not rely on any location information, global synchronization assumptions or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus the overhead of our algorithms is tolerable. Extensive experimental results have verified the effectiveness and the efficiency of DAWN.

EXPERIMENTAL ASSESSMENT OF ABNO-DRIVEN MULTICAST CONNECTIVITY IN FLEXGRID NETWORKS

ABSTRACT

The increasing demand of internet services is pushing cloud services providers to increase the capacity of their data centers (DC) and create DC federations, where two or more cloud providers interconnect their infrastructures. As a result of the huge capacity required for the inter-DC network, the flexgrid optical technology can be used. In such scenario, applications can run in DCs placed in geographically distant locations and hence, multicast-based communication services among their components are required. In this paper, we study two different approaches to provide multicast services in multi-layer scenarios assuming that the optical network is based on the flexgrid technology: *i*) establishing a point-to-multipoint optical connection (light-tree) for each multicast request, and *ii*) using a multi-purpose virtual network topology (VNT) to serve both unicast and multicast connectivity requests. When that VNT is not able to serve an incoming request as a result of lack of capacity, it is reconfigured to add more resources. A control plane architecture based on the Applications-based Network Operations (ABNO) one, currently being standardized by the IETF, is presented; workflows are proposed and PCEP extensions are studied for the considered approaches. The experimental validation is carried-out on a testbed set-up connecting Telefonica, CNIT, and UPC premises**.**

ADAPTIVE EFFICIENT DOWNLINK PACKET SCHEDULING ALGORITHM IN LTE-ADVANCED SYSTEM

ABSTRACT

For a better exploitation of radio resources in the fourth generation networks (4G) Long Term Evolution-Advanced (LTE-A) and for a better guarantee of service quality requested for users, radio resources management and specifically scheduling, play a key role in reaching the objective. In this paper, we propose a new packet scheduling (PS) algorithm for LTE-A downlink transmission that adds a new functionality of an adaptive Time Domain (TD) scheduler to adaptively allocate available resources to GBR (Guaranteed Bit Rate) and NGBR (Non GBR) traffic. Evaluation of our algorithm and comparison with previous works are also presented. The simulation results have demonstrated the effectiveness of our algorithm in terms of the system throughput as well as the delay and the Packet Drop Rate (PDR) for both GBR and NGBR traffic.

DETECTION OF NODE-MISBEHAVIOR USING OVERHEARING AND AUTONOMOUS AGENTS IN WIRELESS AD-HOC NETWORKS

ABSTRACT

In *Wireless Ad-hoc Networks*, nodes co-operate among themselves to forward data packets from a source node to a destination node. Nodes may participate in route discovery or route maintenance process but refuse to forward packets due to presence of faulty hardware or software or to save their resources, such as, battery power and bandwidth. Detection and isolation of misbehavior nodes are important issues to improve the quality of communication service and to save resources of well behaving wireless nodes. In this work, firstly, a neighbor *Overhearing based Misbehavior Detection(OMD)* scheme is proposed. In OMD, each node overhears the transmissions of its neighbors and calculates packet forwarding ratio of its own as well as its neighbors. Source node uses the calculated information to identify a misbehaving node. Secondly, an *Autonomous Agent based Misbehavior Detection(AAMD)* technique is proposed. In AAMD, past behavior of nodes in the network is used as a metric to calculate the selection probability of a node. An agent residing at a node is activated using the activation key generated by a trusted third party to verify the misbehavior of the node. The proposed schemes reduce communication overheads and identification delays to detect misbehaving nodes in wireless ad-hoc network. Simulation results are presented to evaluate the performance of the proposed OMD and AAMD schemes.

IMPROVING THE NETWORK LIFETIME OF MANETS THROUGH COOPERATIVE MAC PROTOCOL DESIGN

ABSTRACT

Cooperative communication, which utilizes nearby terminals to relay the overhearing information to achieve the diversity gains, has a great potential to improve the transmitting efficiency in wireless networks. To deal with the complicated medium access interactions induced by relaying and leverage the benefits of such cooperation, an efficient Cooperative Medium Access Control (CMAC) protocol is needed. In this paper, we propose a novel cross-layer distributed energy-adaptive location-based CMAC protocol, namely DEL-CMAC, for Mobile Ad-hoc NETworks (MANETs). The design objective of DEL-CMAC is to improve the performance of the MANETs in terms of network lifetime and energy efficiency. A practical energy consumption model is utilized in this paper, which takes the energy consumption on both transceiver circuitry and transmit amplifier into account. A distributed utility-based best relay selection strategy is incorporated, which selects the best relay based on location information and residual energy. Furthermore, with the purpose of enhancing the spatial reuse, an innovative network allocation vector setting is provided to deal with the varying transmitting power of the source and relay terminals. We show that the proposed DEL-CMAC significantly prolongs the network lifetime under various circumstances even for high circuitry energy consumption cases by comprehensive simulation study.

WIRELESS COMMUNICATIONS UNDER BROADBAND REACTIVE JAMMING ATTACKS

ABSTRACT

A reactive jammer jams wireless channels only when target devices are transmitting; Compared to constant jamming, reactive jamming is harder to track and compensate against [2], [42]. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) have been widely used as countermeasures against jamming attacks. However, both will fail if the jammer jams all frequency channels or has high transmit power. In this paper, we propose an anti-jamming communication system that allows communication in the presence of a broadband and high power reactive jammer. The proposed system transmits messages by harnessing the reaction time of a reactive jammer. It does not assume a reactive jammer with limited spectrum coverage and transmit power, and thus can be used in scenarios where traditional approaches fail. We develop a prototype of the proposed system using GNURadio. Our experimental evaluation shows that when a powerful reactive jammer is presence, the prototype still keeps communication, whereas other schemes such as 802.11 DSSS fail completely.

A DISTRIBUTED Q LEARNING SPECTRUM DECISION SCHEME FOR COGNITIVE RADIO SENSOR NETWORK

ABSTRACT

Cognitive spectrum management can improve the utilization efficiency of spectrum while increasing the energy consumption of sensor network nodes. Hence, how to balance the energy consumption and spectrum efficiency has become a critical challenge in the resource-constrained cognitive radio sensor networks. In this paper, by analyzing the channel characteristics and the energy efficiency of networks, a joint channel selection and power control spectrum decision algorithm based on distributed Q learning is proposed. To evaluate the performance of the proposed framework, an optimal Q value subject to communication efficiency index is formulated. Then, the learning strategy selection scheme is designed to solve the optimization problem by establishing a learning model. In this learning model, each node can get the strategy of other nodes to select the optimal strategy by introducing distributed strategy estimation. The simulation results show that the proposed algorithm has better performance than the existing methods.

ADAPTIVE DESIGN OPTIMIZATION OF WIRELESS SENSOR NETWORKS USING GENETIC ALGORITHMS

ABSTRACT

We present a multi-objective optimization methodology for self-organizing, adaptive wireless sensor network design and energy management, taking into consideration application-specific requirements, communication constraints and energy-conservation characteristics. A precision agriculture application of sensor networks is used as an example. We use genetic algorithms as the optimization tool of the developed system and an appropriate fitness function is developed to incorporate many aspects of network performance. The design characteristics optimized by the genetic algorithm system include the status of sensor nodes (whether they are active or inactive), network clustering with the choice of appropriate clusterheads and finally the choice between two signal ranges for the simple sensor nodes. We show that optimal sensor network designs constructed by the genetic algorithm system satisfy all application-specific requirements, fulfill the existent connectivity constraints and incorporate energy-conservation characteristics. Energy management is optimized to guarantee maximum life span of the network without lack of the network characteristics that are required by the specific application.

A SENSOR ANONYMITY ENHANCEMENT SCHEME BASED ON PSEUDONYM FOR CLUSTERED WIRELESS SENSOR NETWORK

ABSTRACT

Security problem is an important issue for Wireless Sensor Network. The paper focuses on the privacy protection of WSN applications. An anonymity enhancement tactic based on pseudonym mechanism is presented for clustered Wireless Sensor Network, which provides anonymity for both the sensors within a cluster and the cluster head nodes. Simulation experiments are launched through NS2 platform to validate the anonymity performance. The theoretical analysis and empirical study imply that the proposed scheme based on pseudonym can protect the privacies of both the sensor nodes and the cluster head nodes. The work is valuable and the experimental results are convincible.

AN ENERGY-EFFICIENT MOBILE-SINK PATH SELECTION STRATEGY FOR WIRELESS SENSOR NETWORKS

ABSTRACT

Several studies have demonstrated the benefits of using a mobile sink to reduce the energy consumption of nodes and to prevent the formation of energy holes in wireless sensor networks (WSNs). However, these benefits are dependent on the path taken by the mobile sink, particularly in delay-sensitive applications, as all sensed data must be collected within a given time constraint. An approach proposed to address this challenge is to form a hybrid moving pattern in which a mobile-sink node only visits rendezvous points (RPs), as opposed to all nodes. Sensor nodes that are not RPs forward their sensed data via multihopping to the nearest RP. The fundamental problem then becomes computing a tour that visits all these RPs within a given delay bound. Identifying the optimal tour, however, is an NP-hard problem. To address this problem, a heuristic called weighted rendezvous planning (WRP) is proposed, whereby each sensor node is assigned a weight corresponding to its hop distance from the tour and the number of data packets that it forwards to the closest RP. WRP is validated via extensive computer simulation, and our results demonstrate that WRP enables a mobile sink to retrieve all sensed data within a given deadline while conserving the energy expenditure of sensor nodes. More specifically, WRP reduces energy consumption by 22% and increases network lifetime by 44%, as compared with existing algorithms.

EFFICIENT PACKET PROCESSING AND OPTIMIZATION METHODOLOGIES IN ROUTING PROTOCOLS OF GREEN NETWORKING

ABSTRACT

In the current network environment it is difficult to resolve the problems in network performance. By increasing the performance of energy oriented networking applications, a new network approach is introduced called, Green Networking. Some streaming analysis and measurements are created for preventing the energy streams in architecture. Traditional packet processing engine method is used to represent the most energy saving components of network devices and maintain the traffic overload. The main contribution of this system is to control the power configuration of pipelines and efficiently maintain the traffic flow in heavy traffic networks. To exactly prove the energy aware index solutions in green network a new analytical model is proposed, that model carry out by means of energy aware software routers loaded by real-world traffic traces. The attained consequences reveal how the proposed model can effectively represent energy and network aware performance indexes. The course of action intend at energetically get used to the energy aware device configuration to diminish energy expenditure, while coping with incoming traffic volumes and meeting network performance restriction.

LTE-ADVANCED HETNET INVESTIGATIONS UNDER REALISTIC CONDITIONS

ABSTRACT

With the exponential growth in traffic demands during past years, Heterogeneous Networks (HetNets) are envisioned as the major capacity and performance enhancement enablers by means of increasing the spectral efficiency per unit area. Several multi-cell cooperation techniques have been developed in order to improve the performance of HetNets, such as Range Extension (RE) and enhanced Inter-Cell Interference Coordination (eICIC) for co-channel deployments and inter-site carrier aggregation (CA) for dedicated deployments. The main objective of this study is to analyze the performance of different multi-cell cooperation techniques in a site-specific scenario (central London area) as compared to the case without multi-cell cooperation. The performance of these multi-cell cooperation techniques has been well studied in 3GPP scenarios. But in the site-specific scenario, both the traffic distribution and network layout are far more irregular than in 3GPP scenarios, which calls for a deeper study considering local characteristics.

For co-channel deployment, dynamic algorithms used for cell selection and interference management are proposed in order to adaptively adjust the configurations (RE + eICIC) according to the local characteristics (such as the load and interference conditions). The results show that the performance with dynamic algorithms is much better than with static algorithms, achieving an overall user throughput gain up to 120% and 47% over the static configuration for the 5th and 50th percentile respectively. For dedicated carrier deployment, inter-site CA proves to have good performance in the site-specific scenario, providing an overall user throughput gain up to 100% and 28% for the 5th and 50th percentile respectively, compared to the case without CA. The gain of inter-site CA depends on the UE’s channel quality to both layers (macro layer and small cell layer) and the density of the eNBs of the site-specific scenario.

ON SOCIAL DELAY-TOLERANT NETWORKING: AGGREGATION, TIE DETECTION,AND ROUTING

ABSTRACT

Social-based routing protocols have shown their promising capability to improve the message delivery efficiency in Delay Tolerant Networks (DTNs). The efficiency greatly relies on the quality of the aggregated social graph that is determined by the metrics used to measure the strength of social connections. In this paper, we propose an improved metrics that leads to high-quality social graph by taking both frequency and duration of contacts into consideration. Furthermore, to improve the performance of social-based message transmission, we systematically study the community evolution problem that has been little investigated in the literation. Distributed algorithms based on the obtained social graph are developed such that the overlapping communities and bridge nodes (i.e., connecting nodes between communities) can be dynamically detected in an evolutionary social network. Finally, we take all the results above into our social-based routing design. Extensive trace-driven simulation results show that our routing algorithm outperforms existing social-based forwarding strategies significantly.

PORT-BASED TRAFFIC VERIFICATION AS A PARADIGM FOR ANOMALY DETECTION

ABSTRACT

An *anomaly* is an activity that deviates from the wellknown behaviour of the system. Anomaly detection in networks is of interest from two perspectives: an organization’s perspective and an Internet Service Provider’s (ISP) perspective. Protection of its computer network infrastructure is an important task for all organizations. Organizations desire that their networks are robust and resilient to any kind of attack. Anomaly detection forms an important part of this network resiliency. Also the ISPs want to maximize the utilization of their resources. Hence an ISP would be interested to know any resource failure immediately so as to correct the problem. ISPs would also be interested in safeguarding their network from malicious activities. We describe here a Gaussian Mixture Model (GMM)-based *traffic verification system* as a paradigm for network anomaly detection. The traffic characteristics aggregated over a period of time is given to the model to verify the validity of the traffic. If the traffic does not obey the model then we raise an alarm flagging it as an anomaly. Our results show that the system performs with less than 1% misses and false alarms.

NS2-PROPOSED POTENTIAL SECURITY INFRASTRUCTURE IN VANETS USING TAMPER REGISTERED HARDWARE

ABSTRACT

All over the world many road accidents are occurred due to lack of knowledge of vehicle`s distance and speed. But this issue will be solved by using VANETS through which we can well know about the speed of the vehicle and how much distance it is from other vehicles in all sides. So the VANETS will play a very crucial role in the safety and mostly avoidance of accidents like reacting immediately in dangerous situations. In order to prevent the abuse of VANETS a potential security infrastructure is needed to maintain confidential requirements like message integrity & availability. To achieve this we have proposed a concept called A separate Potential security infrastructure facilitated with symmetric & Asymmetric cryptography with TRH. Our proposed theory will give very high efficient in terms of Computational Needs for the VANETS users.

SECURE SOURCE-BASED LOOSE SYNCHRONIZATION (SOBAS) FOR WIRELESS SENSOR NETWORKS

ABSTRACT

We present the Secure source-based Loose Synchronization (SOBAS) protocol to securely synchronize the events in the network, without the transmission of explicit synchronization control messages. In SOBAS, nodes use their local time values as a onetime dynamic key to encrypt each message. In this way, SOBAS provides an effective dynamic en-route filtering mechanism, where the malicious data is filtered from the network. With SOBAS, we are able to achieve our main goal of synchronizing events at the sink as quickly, as accurately, and as surreptitiously as possible. With loose synchronization, SOBAS reduces the number of control messages needed for a WSN to operate providing the key benefits of reduced energy consumption as well as reducing the opportunity for malicious nodes to eavesdrop, intercept, or be made aware of the presence of the network. Albeit a loose synchronization per se, SOBAS is also able to provide 7:24 _s clock precision given today's sensor technology, which is much better than other comparable schemes (schemes that do not employ GPS devices). Also, we show that by recognizing the need for and employing loose time synchronization, necessary synchronization can be provided to the WSN application using half of the energy needed for traditional schemes. Both analytical and simulation results are presented to verify the feasibility of SOBAS as well as the energy consumption of the scheme under normal operation and attack from malicious nodes.

SPECTRAL AND ENERGY EFFICIENCY ANALYSIS FOR COGNITIVE RADIO NETWORKS

ABSTRACT

Cognitive radio (CR) is considered one of the prominent techniques for improving the utilization of the radio spectrum. A CR network (i.e., secondary network) opportunistically shares the radio resources with a licensed network (i.e., primary network). In this work, the spectral-energy efficiency trade-off for CR networks is analyzed at both link and system levels against varying signal-to-noise ratio (SNR) values. At the link level, we analyze the required energy to achieve a specific spectral efficiency for a CR channel under two different types of power constraint in different fading environments. In this aspect, besides the transmit power constraint, interference constraint at the primary receiver (PR) is also considered to protect the PR from a harmful interference. Whereas at the system level, we study the spectral and energy efficiency for a CR network that shares the spectrum with an indoor network. Adopting the extreme-value theory, we are able to derive the average spectral and energy efficiency of the CR network. It is shown that the spectral efficiency depends upon the number of the PRs, the interference threshold, and how far the secondary receivers (SRs) are located. We characterize the impact of the multi-user diversity gain of both kinds of users on the spectral and energy efficiency of the CR network. Our analysis also proves that the interference channels (i.e., channels between the secondary transmitter and PRs) have no impact on the minimum energy efficiency.

VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS AD-HOC SENSOR NETWORKS

ABSTRACT

Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.