Impregnable Payment Scheme with less translation data and Alter top for Multihop satellite Networks

Mr. P. Srinivasu[1] and Mr. K.N. Brahmaji Rao[2]

1. *Final Year M.Tech, Department of CSE, Baba Institute of Technology and Sciences, Visakhapatnam, AP, India.*
2. *Associate Professor, Department of CSE, Baba Institute of Technology and Sciences Visakhapatnam, AP, India*

Abstract: Multihop wireless networks (MWNs) composed of two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another, without using any kind of fixed wired infrastructure. Multihop wireless networks utilize multiple wireless nodes to provide coverage to a large area by forwarding and receiving data wirelessly between the nodes. In this paper will describe secure transmission of packets with low communication and processing overhead for multihop wireless networks. Receipt based scheme is used in existing system, packet transmission details are does not updated. So, we do not identified cheater node. During this problem we propose RACE, report based payment scheme will have the accounting center. In this scheme each and every state of secure payment will updated. The Evidences are generated for identifying valid and cheating node. A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network (WSAN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Introduction

Multi-hop wireless networks have been studied since 70's . Several new applications of such networks have recently emerged. Community wireless networks are multi-hop wireless networks that provide \last-mile" access to peoples' homes. This approach is an alternative to to cable modem and DSL technologies. In large networks of sensors [10] the scale and the environment are such that a multi-hop wireless network is the only feasible means of communication. A fundamental issue in multi-hop wireless networks is that performance degrades sharply as the number of hops traversed increases. For example, in a network of nodes with identical and omni directional radio ranges, going from a single hop to 2 hops halves the throughput because wireless interference dictates that only one of the 2 hops can be active at a time. The performance challenges of multi-hop networks have long been recognized and have led to a lot of research on the medium access control (MAC), routing, and transport layers of the networking stack. In recent years, there has also been a focus on the fundamental question of what the optimal capacity of a multi-hop wireless network is. The seminal paper by Gupta and Kumar [16] showed that in a network comprising of n identical nodes, each of which is communicating with another node, the throughput capacity per node is 1 pn log n) assuming random node placement and communication pattern and (1 pn) assuming optimal node placement and communication pattern. Subsequent work has considered

alternative models and settings, such as the presence of relay nodes and mobile nodes, and locality in inter-node communication, and their results are less pessimistic [13, 20, 12]. This paper also deals with the problem of computing the optimal throughput of a wireless network. However, a key distinction of our work from previous work such as [16] is that we work with any given wireless network conguration and workload specied as inputs. In other words, the node locations, ranges, etc. as well as the traÆc matrix indicating which source nodes are communicating with which sink nodes are specied as the input. We make no assumptions about the homogeneity of nodes with regard to radio range or other characteristics, or regularity in communication pattern. This is in contrast to previous work that has focused on asymptotic bounds under assumptions such as node homogeneity and random communication patterns.

Related Works:

The existing payment schemes can be classified into tamper-proof-device (TPD)-based and receipt-based schemes. In TPD-based payment schemes, a TPD is installed in each node to store and manage its credit account and secure its operation. For receipt-based payment schemes, an offline central unit called the accounting center stores and manages the nodes' credit accounts. The nodes usually submit undeniable proofs for relaying packets, called receipts, to the AC to update their credit accounts.

Claws of Related Works:

- False accusations and missed detections
- Vulnerable to Collusion attacks
- Long time to identify cheaters.

Relevant Method:

In this paper, we propose RACE, a Report-based payment scheme for MWNs. The nodes submit lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports with almost no cryptographic operations or computational overhead. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credits or pay less. In other words, the Evidences are used to resolve disputes when the nodes disagree about the payment. Instead of requesting the Evidences from all the nodes participating in the cheating reports, RACE can identify the cheating nodes with submitting and processing few Evidences. Moreover, Evidence aggregation technique is used to reduce the storage area of the Evidences.

In RACE, Evidences are submitted and the AC applies cryptographic operations to verify them only in case of cheating, but the nodes always submit security tokens, e.g., signatures, and the AC always applies cryptographic operations to verify the payment in the existing receipt based schemes. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested.

Gratification of Relevant work:

Widespread cheating actions are not expected in civilian applications because the common users do not have the technical knowledge to tamper with

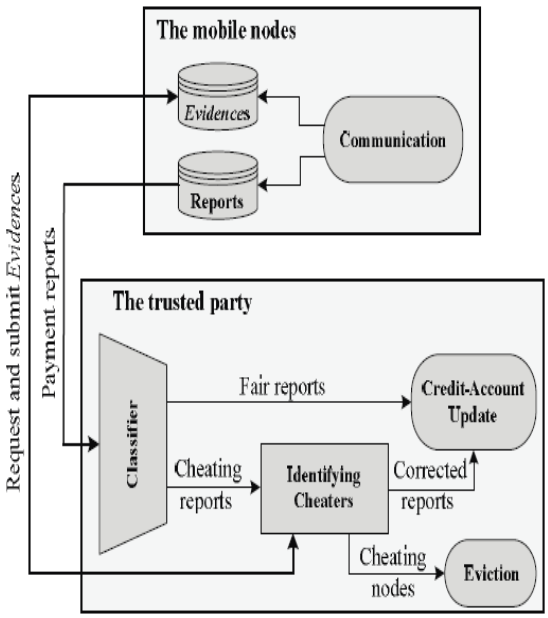
their devices. Moreover, cheating nodes are evicted once they commit one cheating action and it is neither easy nor cheap to change identities. Our analytical and simulation results demonstrate that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and Evidences' storage area, which is necessary to make the practical implementation of the payment scheme effective. Moreover, RACE can secure the payment and precisely identify the cheating nodes without false accusations or stealing credits. To the best of our knowledge, RACE is the first payment scheme that can verify the payment by investigating the consistency of the nodes' reports without systematically submitting and processing security tokens and without false accusations. RACE is also the first scheme that uses the concept of Evidence to secure the payment and requires applying cryptographic operations in clearing the payment only in case of cheating.

In Overall We Summarize:

- Lightweight payment reports (charges and rewards) without security proof
- Almost no cryptographic operations in clearing payments of fair reports
- Uses Evidences to solve disputes
- Reduce storage via Evidence aggregation technique

The Proposed Race:

RACE has four main phases. In Communication phase, the nodes are involved in communication sessions and Evidences and payment reports are composed and temporarily stored. The nodes accumulate the payment reports and submit them in batch to the TP. For the Classifier phase, the TP classifies the reports into fair and cheating. For the Identifying Cheaters phase, the TP requests the Evidences from the nodes that are involved in cheating reports to identify the cheating nodes. The cheating nodes are evicted and the payment reports are corrected. Finally, in Credit-Account Update phase, the AC clears the payment reports. The present study investigates the question whether the co-activation of both source and target language have an influence on the translator's behavior. A way to measure co-activation is the comparative analysis of the influence of different syntactic realizations of the target language entropy on gaze time and production duration during translation and post-editing. We measure syntactic choice in terms of entropy which quantifies the distribution of different translations realizations of a given source segment. High entropy is an indicator of selection effort related to available options of the final translation out of many different realizations. We investigate the impact of syntactic entropy on cognitive effort. In a first step, as research by Jensen et al. (2010) suggests, source text segments which need reordering yield longer gaze times than segments which do not need reordering. In a second step, based on the assumption that syntax is shared



across languages (Hartsuiker & Pickering 2004), a recently activated syntactic structure is likely to influence subsequent processing, thus "priming" it. Low syntactic entropy of translation choices could, thus, be taken to be a sign of priming. To test the hypothesis whether syntactic choices have an influence on cognitive effort, we compared four datasets comprising translation and post-editing data of the same English source texts translated into Danish, German, Spanish and Hindi. Data was manually annotated for syntactic structure along three relevant features: clause type, valency and voice. Our analyses reveal a positive correlation between syntactic entropy of translation realizations values and gaze as well as production time in all four languages. However, no effect of syntactic entropy could be detected in the post-editing data, suggesting that the post-editors were primed by the MT output

System Architecture:

Translation Based on Data Mining:

The aim of the TDA project is to explore and analyse user activity data which is collected in advanced man-machine communication situations. The TDA project will assess and elaborate methods to produce data-driven user profiles, to investigate differences in communication styles, and to identify patterns of user behavior for more and less successful man-machine communication. Data repositories such as the CRITT TPR-DB will be taken as a basis to analyze concrete and specialized forms of professional man-machine communication such as translators behavior in advanced computer-assisted collaborative production environments.

An introductory PhD summer course on Translation Process Research (TPR) and a one-day workshop will precede the TDA project, in which students get acquainted with peculiarities of the TPR data and data acquisition methods. The TDA project will use exploratory statistical approaches for discovering new features and dependencies in the TPR data, and to formulate hypotheses about the causal relations. Statistical hypothesis tests will be deployed for confirming or falsifying existing hypotheses.

Translation of Data:

Propose a mathematical framework for modeling and analyzing multi-hop control networks designed for systems consisting of multiple control loops closed over a multi-hop (wireless) communication network. We separate control, topology, routing, and scheduling and propose formal syntax and semantics for the dynamics of the composed system, providing an explicit translation of multi-hop control networks to switched systems. We propose formal models for analyzing robustness of multi-hop control networks, where data is exchanged through a multi-hop communication network subject to disruptions. When communication disruptions are long, compared to the speed of the control system, we propose to model them as permanent link failures. We show that the complexity of analyzing such failures is NP-hard, and discuss a way to overcome this limitation for practical cases using compositional analysis. For typical packet transmission errors, we propose a transient error model where links fail for one time slot independently of the past and of other links. We provide sufficient conditions for almost sure stability in presence of transient link failures, and give efficient decision procedures. We deal with errors that have random time span and show that, under some conditions, the permanent failure model can be used as a reliable abstraction. Our approach is compositional, namely it addresses the problem of designing scalable scheduling and routing policies for multiple control loops closed

on the same multi-hop control network. We describe how the translation of multi-hop control networks to switched systems can be automated, and use it to solve control and networking co-design challenges in some representative examples, and to propose a scheduling solution in a mineral floatation control problem that can be implemented on a time triggered communication protocols for wireless networks.

Traffic models demand large amounts of data - some of which are: Traffic network topology, traffic network data, zone-data and trip matrices. GIS is a natural tool for handling most of these data as it can ease the work process and improve the quality control. However, traffic models demand a complex topology not very well covered by the traditional GIS-topology.

The paper describes a number of applications where ArcInfo and ArcView have been used to automate the process of building a traffic network topology. The methodology has been or can be used on a number of full-scale models, from medium sized urban areas to metropolitan areas (Copenhagen, Denmark and Bandung, Indonesia). The paper covers key subjects in the work process which has been eased considerably by using AML and Avenue scripts or by using the information from ArcInfo in external applications:

- Semi-automatic procedures for attaching zones and zone-centroids to the traffic network.
- Methods to handle intersection-data, including automatic generation of node data and turn-data from link-attributes.
- (Geographical) Coordination of road networks and public transport networks.
- Methods for handling many project alternatives in a consistent way at network level.

There are several advantages by implementing traffic models in GIS, since the handling of data is easier and the presentation and quality control of results can be done more easily. For this reason, traffic modeling is maybe the field in traffic planning that has made most use of GIS (see Nielsen, 1995/1). However, traffic models demand a complex topology not very well covered by most GIS-packages. Therefore, GIS has primary been used for displaying results from traffic models and not as an active tool in the work process of building the data foundation for traffic models.

Section 2 of the paper describes a number of applications where ArcInfo and ArcView have been used to automate the process of building a traffic network topology. Some of the key subjects in the work process has been eased considerably by using AML and Avenue scripts, other by further modifications done by external applications on data exported from ArcInfo.

Section 3 discuss how to handle many project alternatives in a consistent way without copying the whole data set/coverage each time. This reduces the amount of redundant data significantly.

Section 4 describes the network topology needed to perform a traffic assignment and how to translate from the GIS' network representation to the needed mathematical graph for the calculations/traffic models.

Section 5 outlines the conclusions and perspectives of the use of GIS-based network in the process of traffic modeling.

Claws in Multihop Network System:

The frequency hopping algorithm provides anti-jamming and electronic counter measures (ECM) functionality. Tactical communications networks need to be multi-hop wireless networks in which switches and endpoints are mobile nodes. In a tactical environment, system performance degrades when switching nodes and/or communication links fail to operate, narrow band electronic jamming is widespread and bandwidth is at a premium. Fast and adaptive algorithms for performance analysis are desirable for optimizing the network. Further, tactical networks commonly use preemptive algorithms to achieve low blocking probabilities for high-priority connections when the loss of equipment or electronic warfare in the battlefield is considerable. Under unfavorable conditions, Adaptive Channel Hopping (ACH) algorithm lets sensors switch to a new operating channel. ACH reduces the channel scanning and selection latency by ordering available channels using link quality indicator measurements and mathematical weights. A lot of research on the hopping algorithms is being done internationally in the public domain and details such as configuring the programme etc are country specific and sensitive in nature. The two crucial characteristics which a robust and survivable TCS should have are:

• The mobility of nodes and switches as compared to the static nature of cellular network infrastructure.

• The ability to hop frequency bands and nodes to provide seamless connectivity and ECMs during times of conflict.

There is no doubt about the criticality of the TCS project but what needs to be understood is the feasibility, timeliness and capability of various players to deliver. In one aspect the complexity of TCS for the Army is higher as compared to other services due to the heterogeneity of sensors, types of nodes from soldier to HQ level and the sheer numbers involved.

Tactical networks serve the trinity of voice, data and video communications and need to be versatile and reliable. Legacy and Internet Protocol (IP) based systems need to talk to each other and to eliminate ‘disconnects’. However, a lack of international standards in communication architecture poses hurdles, especially with the legacy radio systems that were not designed to connect to broad-reaching IP-based networks. If we look at the advanced countries of the world the work on military communication is already in full swing (JTRS in USA and Contact Programmer in France). Till date, the success of these major programmers have a few things in common such as participation and contribution of private sector, use of Commercial off the Shelf Technology(COTS), time bound closure of procurement procedures keeping in mind the criticality of the project and electronics manufacturing and IT delivery self-sufficiency.

There is a requirement to deliver on the timelines specified in order to provide the soldier with the much needed equipment enhancement. Challenges are of spectrum, bandwidth, manufacturing and laws of physics. The effectiveness of other big ticket modernization programmers also depends on the successful implementation of TCS such as the F-INSAS.

The modern communication equipment that is required at the tactical level is as under:

• High Frequency (HF) radio (2-30MHz) – Though prone to unpredictability and unreliability, its key contribution is its beyond-line-of-sight application by refracting signals off the ionosphere for a

fraction of the cost of a SATCOM signal which is finite and overburdened.

• Very HF radio (30-300MHz) - Man-portable tactical internet relies on VHF Combat Net Radios (CNR), particularly at the section/squad level. VHF offers a sizeable frequency range for high-quality signals. Limitation is line of sight (range 8 km) and horizontal integration.

• Ultra HF radio (300-3000MHz)-The gap of horizontal integration is addressed by the recent advent of smaller, handheld UHF Personal Role Radios (PRR) carried by soldiers. Allows soldiers to bypass traditional shouts and hand signals.

India needs to invest in electronics designing and manufacturing to complement the mature software base of our country. Private sector participation is crucial and they have demonstrated their capabilities and have played pivotal roles in some of India's most secret defence projects. Larsen & Toubro built a considerable portion of India's nuclear submarine, INS Arihant. Another private company, Tata Power, which built crucial command systems for the Arihant, also designed the core of the top secret Samyukta Electronic Warfare System. The two algorithms for frequency hopping and encryption can be devised by Centre for Artificial Intelligence and Robotics (CAIR) lab of DRDO as they are of sensitive nature. The application of Micro-electromechanical Systems (MEMS) can address weight and powers issues which are standard but important components of the complex system. Indigenous production of high-capacity, autonomous, distributed switches ready to provide full service just minutes after power-up is crucial to the TCS programme. Keeping in mind future upgrades to the system a Software-Defined Platform able to service various waveforms on a single equipment needs to be developed. As the complexity of the separation process (SIGINT and ELINT) depends on the complexity of the transmission methods (e.g., hopping) state of art algorithms for frequency hopping and encryption need to be devised. International studies have shown that preemption algorithms are the best way to utilise limited resources in a battlefield and to compensate for the loss of equipment; this aspect also needs to be included in the TCS. Use of COTS technology can be highly beneficial as it lowers cost and reduces soldier familiarization time through existing commercial technology.

Modules:

- Route establishment
- Data transmission
- Evidence composition
- Payment report composition/submission

Reference:

A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEEhttp://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6175892

G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous ommunication Protocol for Peer-to-Peer Applications OverMobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications," Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, pp. 255-265, Aug. 2000.

G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey,"Wiley's J. Wireless Comm. and Mobile Computing, vol. 6, no. 3,pp. 319-332, 2006

A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bern, Nov. 2005.

A. Weyland, T. Staub, and T. Braun, "Comparison of Motivation Based Cooperation Mechanisms for Hybrid Wireless Networks," J. Computer Comm., vol. 29, pp. 2661-2670, 2006.

S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof,Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

M. Mahmoud and X. Shen, "FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012.

M. Mahmoud and X. Shen, "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology,vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

A. Menzies, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, www.cacr.math.uwaterloo.ca/hac, 1996.

Nat'l Inst. of Standards and Technology (NIST), "Recommendation for Key Management - Part 1: General (Revised),"Special Publication 800-57 200, 2007.

NIST, "Digital Hash Standard,"Fed. Information Processing Standards Publication 180-1, Apr. 1995.

N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE Trans. Mobile Computing, vol. 5, no. 2, pp. 128-143, Mar./Apr. 2006.

P. Desnoyers, D. Ganesan, H. Li, M. Li, and P. Shenoy, "PRESTO: A Predictive Storage Architecture for Sensor Networks," Proc. 10th Workshop Hot Topics in Operating Systems (USENIX HotOS), June 2005.