EFFICIENT SOLUTION WITH SECURITIES ISSUE FOR ROUTING PROTOCOL IN WIRELESS NETWORK

Prof. Bhagappa[1], Prof. Vijay Anand H. M[2], Prof. Kiran Kumar A[3], Prof. Kemparaju[4]
Visveshwaraya Technological University (VTU), Karnataka

Abstract

We propose a new routing protocol, which is anonymous secure routing (AASR), to satisfy the requirement and defend the attacks. the route request packets are authenticated by a group signature, the potential active attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message, is designed to prevent intermediate nodes from inferring a real destination.

We address fault tolerance in wireless sensor networks .In sensed data streams indicate the spread of malicious attacks, hardware failure and software corruption among the different nodes in a Wireless Sensor Network. we start by providing a short summary of sensor networks and classical fault tolerance techniques in the system, we discuss the three phases of fault tolerance detection and identification at four levels of abstractions (hardware, system software, middleware, and applications) and four scopes . the factors of the node infected can be generated and incoming data streams resulting in chances of inaccurate data misleading packet transmission wrong decision making and server communication disruption.

Wireless sensor network composed of very large number of low cost micro-sensors. A wireless sensor network of the type refer a group of the sensors, or node, that are linked by a wireless medium to perform the distributing the sensing tasks. With the new system like micro-electro-Mechanical system(MEMS) technology taking low power in wireless sensor network communication. Now the big challenge is that to produce the wireless sensor nodes at low cost. The network is used to collect and send the various types of data and message to the destination. The low cost WSN has the limited battery power and the replacing the battery is the not a solution in the network because large nodes will be there.

We consider the scenario in which a large number of sensor nodes are densely deployed and sensor readings are spatially correlated. Now we are proposing the system present a joint source and network coding scheme in that injecting the concept of compression sensing in the network coding which avoid the effect of network decoding, the energy consume by the network is highly unreliable. we present the Reliable Reactive Routing Enhancement (R3E) to increase the resilience to link dynamics for WSNs/IWSNs. R3E is designed to enhance existing reactive routing protocols to provide reliable and energy efficient packet delivery against the unreliable wireless links by utilizing the local path diversity. Specifically, we introduce a biased back off scheme during the route-discovery phase to find a robust guide path, which can provide more cooperative forwarding.

Keywords: Routers, Protocols, Packets, Route discovery algorithms, link, encryption, decryption, sensor, RREQ, RREP,AASR, MANET..etc

Introduction

Based on sensor technology, low-power digital electronics and low-power wireless communication. it is now possible to produce wireless sensor nodes in quantity at low cost Wireless ad hoc network is a collection of autonomous mobile nodes that communicate with each other over wireless links. The

networks are expected to play increasingly important role in future organizations, setting, being useful for providing communication support where no fixed infrastructure exists or the deployment of a fixed infrastructure is not economically profitable and movement of communicating parties is possible. Due to the limited transmission range of wireless network interfaces, multiple networks "hops" may be needed for one node to exchange data with another across the network. A node can move anytime in an ad hoc scenario and, as a result, such as base stations, mobile hosts are need to operate as routers in order to maintain the information and the network connectivity.

The wireless sensor network has the various research in the monitoring application. The detection of the certain event is made viable through the data sensing and forwarding from the sensor node the data sensing and forwarding from sensor node to the called sensor node so called sink node for further processing. Wireless sensor networks themselves are a new scientific and engineering field and it is not still quiet clear as to what is the best way to address a particular problem. it is also difficult to accurately predict the best way to treat fault tolerance within a particular wireless sensor network approach. The detection of certain events is made vital through the data sensing and forwarding from the sensor node to the sink node for the further processing. The energy constraints and other resource limitations restrict direct communication between sensor and sink node. Communication in the wireless sensor network is affected by the proper functionality and various nodes have the intermediate node. The occurrence of any unexpected circumstance and resources limitations restrict redirect communication between sensor and sink node.

Recent advances in micro-electro-mechanical systems (MEMS) and low power and highly integrated digital electronics have led to the development of micro sensors. Such sensors are generally equipped with data processing and communication capabilities. The sensing circuitry measures ambient conditions related to the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. The sensor sends such collected data, usually via radio transmitter, to a command center (sink) either directly or through a data concentration center (a gateway). The decrease in the size and cost of sensors, resulting from such technological advances, has fueled interest in the possible use of large set of disposable unattended sensors. we propose a General Self-Organized Tree based Energy Balance routing protocol (GSTEB).We consider a situation in which the network collects information periodically from a terrain where each node continually senses the environment and sends the data back to BS .

Wireless Sensor Network (WSN) is used for monitoring and recording the physical conditions of the environment and communicate the information gathered from the monitored field through wireless links. A sensor network consists of a collection of few hundreds to thousands sensor nodes which can perform some specific action and are battery powered. Compared to other wireless networks. sensor nodes have become small, inexpensive, low-power and distributed. Sensor networks have been useful in many fields like military, health, monitoring. Wireless sensor networks are replacing wired industrial application, communication since the industrial wireless sensor network. IWSN applications, such as factory automation industrial process monitoring.

Objective

- We focus on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes.
- We need to propose authenticated anonymous secure routing (AASR) to overcome the pre-mentioned problems.
- We adopt a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage
- Need to develop the method that can by-pass infected areas and make the transmission to the unaffected area.
- To minimize the aforesaid serve effects of infected nodes. The problem does not appear to be too complicated and the effect of trapping important packets an infected region could be massive.

- To find a solution that can mitigate the aforesaid problems and get the stuck packets out of infected regions.
- N sensor nodes are randomly distributed in the square field and there is only one BS deployed far away from the area.
- Sensor nodes are stationary and energy constrained. Once deployed, they will keep operating until their energy is exhausted.
- BS is stationary, but BS is not energy constrained.
- We consider the effect of route discovery on the cooperative forwarding performance and combine the solutions to reliable route discovery and efficient cooperative forwarding problems.
- We propose a simple yet effective cooperative forwarding scheme. Along the discovered virtual path, data packets can be greedily forwarded toward the destination through nodes' cooperation without utilizing location information.

Literature survey

[5]. An Anonymity-Based Secure On-Demand Routing for Mobile Ad Hoc Networks

Privacy and Security have emerged as an important research issue in Mobile Ad Hoc Networks (MANET) due to its unique nature such as scarce of resources and absence of centralized authority. There are number of protocols have been proposed to provide privacy and security for data communication in an adverse environment, but those protocols are compromised in many ways by the attackers. The concept of anonymity (in terms of unlinkability and unobservability) and pseudonymity has been introduced in this paper to ensure privacy and security. In this paper, a Secure Onion Throat (SOT) protocol is proposed to provide complete anonymity in an adverse environment. The SOT protocol is designed based on the combination of group signature and onion routing with ID-based encryption for route discovery.

Advantage

- Secure Onion Throat protocol provides privacy and security for data communication through complete anonymity in mobile ad hoc networks.
- SOT prevents strong eavesdroppers, from exposing local wireless transmitters' identities

Disadvantage

- Provides anonymity only during route discovery and data forwarding.
- Besides route discovery and data forwarding anonymity is also required during event reporting

[5]. Minimizing Recovery State In Geographic Ad-Hoc Routing

Geographic ad hoc networks use position information for routing. They often utilize stateless greedy forwarding and require the use of recovery algorithms when the greedy approach fails. We propose a novel idea based on virtual repositioning of nodes that allows to increase the efficiency of greedy routing and significantly increase the success of the recovery algorithm based on local information alone. We explain the problem of predicting dead ends which the greedy algorithm may reach and bypassing voids in the network, and introduce NEAR, Node Elevation Ad-hoc Routing, a solution that incorporates both virtual positioning and routing algorithms that improve performance in ad-hoc networks containing voids. We demonstrate by simulations the advantages of our algorithm over other geographic adhoc routing solutions.

Advantage

1. Improve performance, based on local information alone.
2. The shape of voids can be smoothed and concave nodes can be predicted by their added virtual height.

Disadvantage

1. There is a gateway for future research where the nodes room the network.
2. The effect of snapping has not been considered

[2]. Wireless sensor network survey

A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, cost, hardware,

and system constraints We classify the problems into three different categories: (1) internal platform and underlying operating system, (2) communication protocol stack, and (3) network services, provisioning, and deployment.

Advantage

- The potocol only consumes 1.5% to 15% power of 10% S-MAC.
- Collision free for data traffic, Yields in reliable transmission

Disadvantages

- The time for TDMA-W to compute a reduction is much higher than S-MAC
- For broadcast operation traffic the reliable transmission can't be generated in S-MAC

[2]. Guaranteeing Real-Time Services for Industrial Wireless Sensor Networks with IEEE 802.15.4

Industrial applications of Wireless Sensor Networks require timeliness in exchanging messages among nodes. Although IEEE 802.15.4 provides a superframe structure for real-time communication, a real-time message scheduling algorithm is still required to schedule a large number of real time messages to meet their timing constraints. We propose a distance constrained real-time off-line message scheduling algorithm which generates the standard specific parameters such as BO, SO and GTS information and allocates each periodic real-time message to super frame slots for a given message set. The proposed scheduling algorithm is evaluated and analyzed extensively through simulations. In addition, a guaranteed time service is
implemented in a typical industrial sensor node platform with a well-known IEEE 802.15.4 compliant transceiver.

Advantages

- The implemented system runs accurately according to the schedule generated by the proposed algorithm.

Disadvantage

- IEEE 802.15.4 provides GTS for real-time messages, but it has limitations.
- There is a future gateway that includes the extension of the scheduling algorithm for on-line scheduling and frequency hopping

Methodology

Module 1: AASR: Authenticated Anonymous Secure Routing for MANETs in dversarial Environments

- Anonymity and Security Primitives
- Anonymous On-demand Routing Protocols
- Anonymous Data Transmission

Module 2: By-Passing Infected Areas in Wireless Sensor Networks using BPR

- **Fuzzy Data Clustering**
  - Avoiding Infected Areas
- **By-Passed Routing (BPR)**
  - The Twin Rolling Balls
  - The Exit Gate Node
- **Traffic Diversion**
- **Beacon Updates**
  - Normal Forwarding Algorithm

Module 3: A General Self-Organized Tree-Based Energy-Balance Routing Protocol for Wireless Sensor Network

General self-organized tree-based energy-balance routing protocol.

- Tree Constructing Phase
- Self-Organized Data Collecting and Transmitting Phase
- Information Exchanging Phase

Module 4: R3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks

- Reliable Guide Path Discovery
- Route Request (RREQ) Propagation:
  - handles the RREQ received from node
- Route Reply (RREP) Propagation
  - handles the RREP received from its downstream guide node
- Cooperative Forwarding

Proposed System

we focus on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes. We assume that there is no online security or localization service available when the network is deployed. We propose an authenticated anonymous secure routing (AASR) to overcome

the pre-mentioned problems. We adopt a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.

The proposed By-Passed Routing (BPR) technique comprises two main parts, namely Infected area detection and by-passed routing. The first part detects the occurrence of infected nodes adapting a Fuzzy Data Clustering approach to identify anomalies based on the received data signals. The fuzzy clustering method is chosen as it provides an unsupervised and modular method for evaluating anomalous data over the different sensor nodes.

The information about infected nodes is then directly used for traffic diversion in the proposed BPR technique. The novelty of the BPR approach relies on the introduction of the simultaneous twin rolling balls technique that detects the next 1-hop neighbor faster than the existing GAR approach. Using this approach, the first node that hits any ball in any direction and is uninfected is assigned as the next hop. A further different way of getting the stuck packets out of infected regions is another unique contribution of BPR.

we propose a General Self-Organized Treebased Energy Balance routing protocol (GSTEB).We consider a situation in which the network collects information periodically from a terrain where each node continually senses the environment and sends the data back to BS.

The time from the start of the network operation to the death of the first node in the network. b) The time from the start of the network operation to the death of the last node in the network, we adopt the first definition. Moreover, we consider two extreme cases in data fusion

In IWSNs, transmission failures can result in missing or delaying of process or control data, and missing the process or control deadline is normally intolerable for industrial applications, as it may cause chaos in industrial automation or possibly terminate the automation, ultimately resulting in economic losses . The sensed data should be reliably and timely transmitted to the sink node, and the programming or retasking data for sensor node operation, command, and query should be reliably delivered to the target nodes. It is also required that these networks can operate for years without replacing the device batteries. Therefore, the reliability, timeliness, and energy efficiency of data forwarding are crucial to ensure proper functioning of an IWSN. However, one of the major technical challenges for realization of IWSNs is to provide reliable and efficient communication in dynamic and harsh environments. This is because, in harsh industrial environments, sensor nodes may be subject to radio frequency (RF) interference, highly caustic or corrosive environments, high humidity levels, vibrations, dirt and dust, or other conditions that challenge network performance.

Advantage

- When a node faces congestion, it attempts to inform the source node from which it receives packets with the lowest data rate, to suppress its data rate
- He process is reverse and begins from the nodes that communicate directly with the sink.
- It adjusts its data rate and simultaneously adds a specific bit in each packet header it transmits indicating that its data rate is throttled
- Proposed by-passed routing (BPR) avoids infected areas and its efficacy to improve the overall performance.
- We have solved three major dilemmas in the traditional routing approaches: local minima, false boundary detection and visits to unnecessary nodes.
- Exhibits high performance compared with the other studied protocols, BOUND HOLE & GAR.
- The proposed twin rolling balls greatly help to define the next forwarding node and mitigate the false boundary detection applicable in the existing rolling ball technique
- Each packet sent to the parent nodes will be fused, the minimum energy consumption can be achieved if each node chooses the node nearest to it.
- We can find that some clusters are formed, but they cannot connect with others. Thus in GSTEB, we use criterion to limit the search direction.

- Each node knows the ID of its parent node. In each time slot, in order to reduce communication interference, we apply FHSS in which each child node communicates with its parent node using the frequency hopping sequence determined by its parent node ID.

Conclusion

We design a anonymous network need to implement MANET network in the adversarial network in the systemThe route request packets are authenticated by group signatures, which can defend the potential active anonymous attacks without unveiling the node identities. proposed By-Passed Routing (BPR) in avoiding infected areas and its efficacy in improving the overall performance. The infected areas are anomalous nodes detected using a fuzzy data clustering method and the information collected is used in the proposed BPR technique. We introduce GSTEB. Two definitions of network lifetime and two extreme cases of data fusion are proposed. when the data collected by sensors is strongly correlative, GSTEB outperforms LEACH, PEGASIS, TREEPSI and TBC. We presented R3E, which can augment most existing reactive routing protocols inWSNs/IWSNs to provide reliable and energy-efficient packet delivery against the unreliable wireless links.

References

[5] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 8, pp. 888– 902, Aug. 2007.

[5] N. Arad and Y. Shavitt, "Minimizing recovery state in geographic ad hoc routing," IEEE Transactions on Mobile Computing, vol. 8, no. 2, pp. 203–217, 2009.

[2]I. F. Akyildiz *et al.*, "Wireless sensor networks: A survey," *Computer Netw.*, vol. 38, pp. 393–422, Mar. 2002.

[4] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. IEEE ICNP*, Nov. 2001, pp. 14–23