International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Enhancing Three-Hop Routing Protocol to Raise the High Throughput and Reducing packet Delay Using wireless Sensor Network

Dr. V. Jayaraj,
Associate Professor,Department Of Computer Science And Engineering,
Bharathidasan University, Trichy
Mrs.S.Hemalatha
Research Scholar, Bharathidasan University, Trichy
G. Revathi
Research Scholar, Department of Computer Science
Shrimati Indira Gandhi College, Trichy,

ABSTRACT:- *A Hybrid wireless network is the combination of both mobile ad-hoc networks and infrastructure wireless networks which is used to improve the performance of our network. The routing protocols are used to combine the ad-hoc transmission mode with the cellular transmission mode. This paper describes a Distributed Multipath Routing Protocol for hybrid wireless networks which establishes multiple paths between source and destination. , we reveal the in efficient use of watchdog technique in existing trust systems, and propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system's security in a sufficient level. It reduces overhead and path loss. It also has a congestion control algorithm to avoid traffic among the base stations. The analysis results show that this protocol can able to increase the ability in terms of throughput.*

Keywords: **Hybrid wireless Network, Three- Hop, Distributing, Throughput, Overhead**

1. INTRODUCTION

Over the past few years, wireless networks including infrastructure wireless networks and mobile adhoc networks (MANETs) have attracted significant research interest. The growing desire to increase wireless network capacity for high performance applications has stimulated the development of hybrid wireless networks. A hybrid wireless network consists of both an infrastructure wireless network and a mobile ad-hoc network. Wireless devices such as smart-phones, tablets and laptops, have both an infrastructure interface and an ad-hoc interface. As the number of such devices has been increasing sharply in recent years, a hybrid transmission structure will be widely used in the near future. Such a structure synergistically combines the inherent advantages and overcome the disadvantages of the infrastructure wireless networks and mobile ad-hoc networks.

Wireless sensor networks are the networks which are formed with a group of devices equipped with sensors distributed in space. These devices are used to measure and record various environmental conditions in diverse locations. A sensor network is made of sensor nodes where each sensor node is equipped with a radio transceiver along with an antenna, a microcontroller, an interfacing electronic circuit and an energy source (usually a battery). Each sensor node can be imagined as a small computer consisting of a processing unit and a limited amount of computational power and memory. The main difference between the Wireless Sensor Networks (WSNs) and adhoc networks is that for WSNs, the main functions are monitoring and collecting the data whereas for the adhoc networks, the main focus is on communication aspects.

2. LITERATURE SURVEY

ENERGY EFFICIENT TOPOLOGIES FOR WIRELESS SENSOR NETWORKS

A wireless network is a group of spatially dispersed specialized transducers with a sensing, computing and communication infrastructure which intends to give them the ability to sense and record various conditions in a monitored environment. They act as interfaces between real and virtual worlds. They are the most rapidly developing information technologies in today's world due to their vast range of applications. This paper gives an overview of wireless sensor networks and provides a scenario

based comparison for energy efficiency between different topologies used in these networks.

GROUP-BASED TRUST MANAGEMENT SCHEME FOR CLUSTERED WIRELESS SENSOR NETWORKS

Traditional trust management schemes developed for wired and wireless ad hoc networks are not well suited for sensor networks due to their higher consumption of resources such as memory and power. In this work, we propose a new lightweight Groupbased Trust Management Scheme (GTMS) for wireless sensor networks, which employs clustering. Our approach reduces the cost of trust evaluation. Also, theoretical aswellassimulationresultsshowthatourschemedemandslessmemory,energy,andcommunication overheads as compared to the current state-of-the-art trust management schemes and it is more suitable for large-scale sensor networks. Furthermore, GTMS also enables us to detect and prevent malicious, selfish, and faulty nodes.

TWO-FACTOR USER AUTHENTICATION IN WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSN) are typically deployed in an unattended environment, where the legitimate users can login to the network and access data as and when demanded. Consequently, user authentication is a primary concern in this resource-constrained environment before accessing data from the sensor/gateway nodes. In this letter, we present a two-factor user authentication protocol for WSN, which provides strong authentication, session key establishment, and achieves efficiency

EVOLUTIONARY AND PRINCIPLED SEARCH STRATEGIES FOR SENSORNET PROTOCOL OPTIMIZATION

Interactions between multiple tunable protocol parameters and multiple performance metricsaregenerally complex and unknown; finding optimal solutions is generally difficult. However, protocol tuning can yield significant gains in energy efficiency and resource requirements, which is of particular importance for sensornet systems in which resource availability is severely restricted. We address this multi-objective optimization problem for two dissimilar routing protocols and by two distinct approaches. First, we apply factorial design and statistical model fitting methods to reject insignificant factors and locate regions of the problem space containing near-optimal solutions by principled search. Second, we apply the Strength Pareto Evolutionary Algorithm 2 and Two-Archive evolutionary algorithms to explore the problemspace, with eachiteration potentially yielding solutions of higher quality and diversity thanth eprecedingiteration.Whereas a principled search methodology yields a generally applicable survey of the problem space and enables performance prediction, the evolutionary approach yields viable solutions of higher quality and at lower experimental cost. This is the first study in which sensornet protocol optimization has been explicitly formulated as a multi-objective problem and solved with state-of-the-art multiobjective evolutionary algorithms.

3. **Existing System**

As a critical complement to traditional security mechanisms (e.g., cryptographic methods , authentication and access control logics etc.), trust systems are widely applied to protect wireless sensor networks (WSNs for short) from being attacked by "legitimate" sensor nodes (i.e., the nodes are either compromised or selfish or on fault) . Those nodes can bypass traditional security protections using their "legitimate" identities, but can be possibly captured by trust systems due to their poor reputation or past misbehavior . That is, trust is built upon sensor nodes' reputation and past behaviors, and can be used to model these nodes' honesty and internal states. Although many trust systems enable trust recommendations to extend the trust from neighborhood (i.e., direct trust) to a global network view (i.e., indirect trust), the direct experience of past behaviors is still the basis for securing those recommendations. In another word, sensor nodes' past behaviors constitute the basic foundation for building WSN's trust systems (WSNTSs for short).

Drawbacks of Existing System

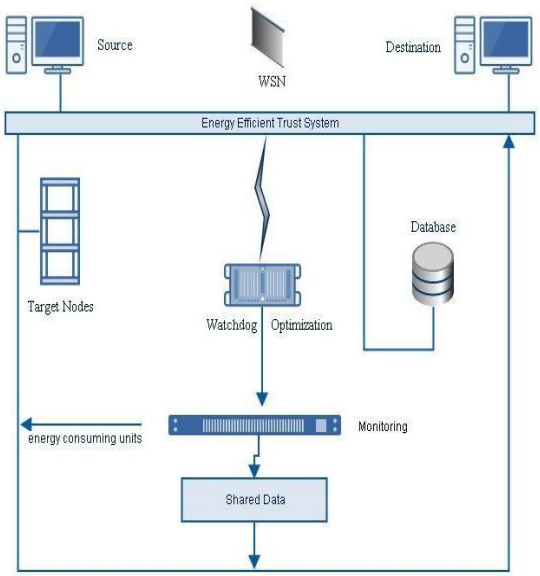
- WSN may lack a wide variety of business traffic to build up all kinds of trust
- Watchdog technique has been proved as a very effective approach to build up WSNTS's foundations, it introduces a large amount of additional energy consumptions which conflict the energy efficient design principle of WSN

PROPOESD SCHEME

In this paper, we will fill in this gap by optimizing watchdog techniques for WSNTSs to balance energy efficiency and security (in terms of trust accuracy and robustness). Our ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. To touch this goal, we optimize watchdog techniques in two levels. First, we optimize watchdog locations by considering the fact: although sensor nodes which are located more closely may consume less energy to monitor each other due to shorter communication distance , these nodes are more likely of being compromised together and

launch collaborative attacks .We therefore explore the optimal watchdog location (given a target node) to minimize the overall risk (in terms of both energy consumption and security). Second, we optimize watchdog frequency and reduce its redundancy. In particular, compared with the sensor nodes whose behaviors are more uncertain, the nodes with more determined trustworthiness (i.e., trustworthy or untrustworthy) may require less watchdog tasks (i.e., lower watchdog frequency) to further investigate.

4. SYSTEM MODEL



Trust System

Client-server computing or networking is a distributed application that partitions watchdog's task between source and target nodes. Often clients and servers operate over a network on separate functionalities. A server machine is a high-performance host that is running one or more tasks which share its resources with nodes.

Watchdogs Technique

All the active nodes in WSN, Once the correct destination router is found, an end-to-end peer connection (TCP or IP) is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use, permitting casual, any-to-any communication without the burden of specifying peer connections in advance. When performing watchdog tasks to monitor routing behavior, the watchdog nodes may waste some watchdog tasks if they miss the target node's forwarding packets due to noises.

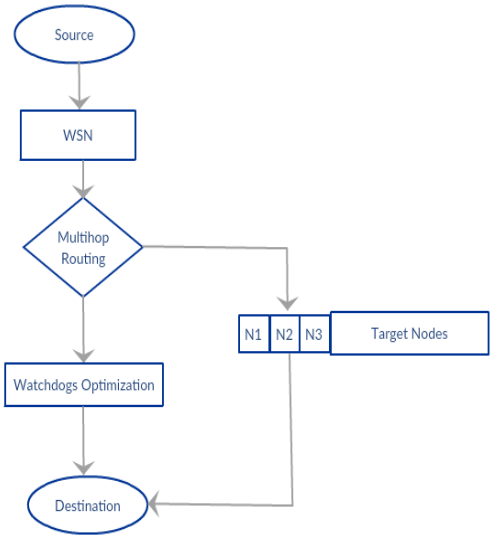
Target Nodes

The number of connections to establish between each pair of target node is established between each and every nodes for network communication. From the source node to the destination node and intermediates node must have connection between source nodes after communicate between combinations of multi node each and every node must be link to each other. In multipath data transmission, send the data from source node that means which type of file size and file extension.

Energy Consumption

In proposed a energy-efficient trust model by applying a geographic target nodes to identify trust managers (may save energy due to low storage usage), while implemented an energy watcher to help sensor nodes estimate their neighbor nodes' energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route. Moreover, a watchdog's technology is widely used to estimate energy consumed by each task typical free space wireless radio model. In this model, a sensor node's transmitter unit to the main node as file request and then the facts can be sends multiple requested node and DBP algorithms to avoid the WSNTS attacks. The source node sends all type of file, and then enters the data sends from source node to destination node over the network. As well as data must be send from source node to intermediate node automatically in this module the data's are successfully transfer from source to destination without attacks.

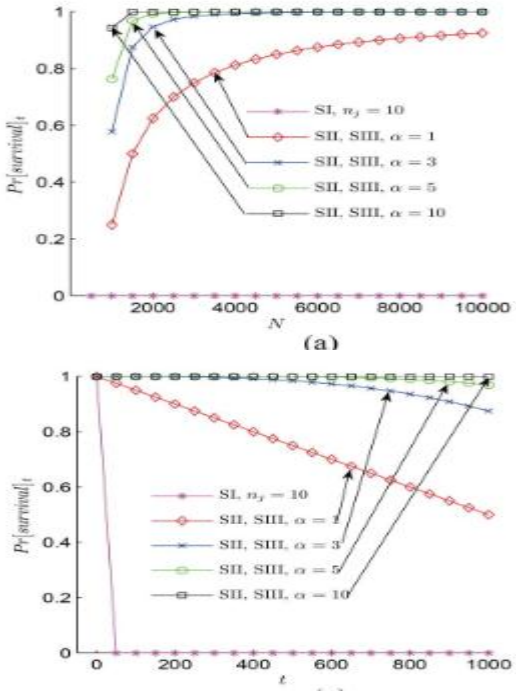
6. FLOWCHART



7. CONCLUSION AND FUTURE WORK

A hybrid wireless network combining an infrastructure wireless network and a mobile ad-hoc network leverages their advantages to increase the throughput capacity of the system. However, current hybrid wireless networks simply combine the routing protocols in the two types of networks for data transmission, which prevents them from achieving higher system capacity. In this paper, we proposed a Distributed Three-hop Routing (DTR) data routing protocol that integrates the dual features of hybrid wireless networks in the data transmission process. In DTR, a source node divides a message stream into segments and transmits them to its mobile neighbors, which further forward the segments to their destination through an infrastructure network. DTR limits the routing path length to three, and always arranges for high-capacity nodes to forward data. Unlike most existing routing protocols, DTR produces significantly lower overhead by eliminating route discovery and maintenance. In addition, its distinguishing characteristics of short path length, short-distance transmission, and balanced load distribution provide high routing reliability and efficiency. DTR also has a congestion control algorithm to avoid load congestion in BSes in the case of unbalanced traffic distributions in networks. we take the step to answer an important research question on whether WSNTS can still maintain sufficient security when the trust's basic foundations (i.e., the first-hand experiences) are minimized. We give out a very positive result to this question through theoretical analysis and extensive experiments. Our studies thus shed light a promising research direction on the design of energy-efficient WSNTS by optimizing the collection procedure of first-hand experiences.

8. Graph:



9. REFERENCES:

[1] H Luo, R. Ramjee, P. Sinha, L. Li, and S. Lu. Ucan: A unified cell and ad-hoc network architecture. In Proc. of MOBICOM, 2003.
[2] P. K. McKinley, H. Xu, A. H. Esfahanian, and L. M. Ni. Unicastbased multicast communication in wormhole-routed direct networks. TPDS, 1992.
[3] H. Wu, C. Qiao, S. De, and O. Tonguz. Integrated cell and ad hoc relaying systems: iCAR. J-SAC, 2001.
[4] Y. H. Tam, H. S. Hassanein, S. G. Akl, and R. Benkoczi. Optimal multi-hop cellular architecture for wireless communications. In Proc. Of LCN, 2006.
[5] Y. D. Lin and Y. C. Hsu. Multi-hop cellular: A new architecture for wireless communications. In Proc. of INFOCOM, 2000.
[6] P. T. Oliver, Dousse, and M. Hasler. Connectivity in ad hoc and hybrid networks. In Proc. of INFOCOM, 2002.
[7] E. P. Charles and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers. In Proc. Of SIGCOMM, 1994.

[8] C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc on demand distance vector (AODV) routing. Technical report, Internet Engineering Task Force, 2003.
[9] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. IEEE Mobile Computing, 1996.
[10] V. D. Park and M. Scott Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proc. Of INFOCOM, 1997.
[11] R. S. Chang, W. Y. Chen, and Y. F. Wen. Hybrid wireless network protocols. IEEE Transaction on Vehicular Technology, 2003.
[12] G. N. Aggelou and R. Tafazolli. On the relaying capacity of nextgeneration gsm cellular networks. IEEE Personal Communications Magazine, 2001.
[13] T. Rouse, I. Band, and S. McLaughlin. Capacity and power investigation of opportunity driven multiple access (ODMA) networks in TDD-CDMA based systems. In Proc. of ICC, 2002.
[14] H. Y. Hsieh and R. Sivakumar. On Using the Ad-hoc Network Model in Wireless Packet Data Networks. In Proc. of MOBIHOC, 2002.