International Journal of Scientific & Engineering Research, Volume 4, Issue 2, February-2013
ISSN 2229-5518

Secure Routing Using Trust Based Mechaniam in Wireless Sensor Networks(WSNs)

Mrs.S.Devisri, Mr.C.Balasubramaniam

Abstract—. *Wireless Sensor Networks (WSN) are a most challenging and emerging technology for the research. Today wireless sensor networks are broadly used in environmental control, Surveillance tasks, maintaining tracking and controlling etc. On the top of all this the wireless Sensor Networks need very secure communication. Ensuring confidence between every pair of interacting nodes is important in this type of networks .This paper introduce a new framework for the formation of trustworthy route from source node to Base Station(BS) for secure routing of messages in Wireless Sensor Networks.*

Index Terms— Base Station (BS). Dynamic Source Routing, Security, Trust Worthy, Wireless Sensor Networks (WSNs)

1 INTRODUCTION

Wireless sensor networks (WSNs) are used in many applications in military, ecological, and health related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in building. Security is therefore important in WSNs. However, WSNs suffer from many constrains, including low computation capability, small memory, limited energy resources, susceptibility to physical capture , and the use of in secure wireless communication channels. These constraints make security on WSNs a challenge.

Wireless Sensor Networks are collection of nodes has its own sender, processor, transmitter and receiver and such sensors usually are low cast devices that perform a specific type of sensing task.

Being of low cost , such sensors are deployed densely through the area to monitor specific event. The Wireless Sensor Networks mostly operate in public and uncontrolled area and the security is the major challenges in sensor applications.

The cryptographic security system in WSNs cannot detect the node physical capture the malicious or selfish nodes .Hence, new security systems are required for secure routing of messages from source to BS of WSNs. A new way of getting security without using cryptography is trust based security in WSNs.

- *Mrs.Devisri is currently pursuing masters degree program in computer science and Engg dep in Erode sengunthar Engineeringcollege,Anna University, India, cell-9542416655. E-mail: srisankar8882@gmail.com*
- *Mr.C.Balasubramaniam is currently working as a lecturer in Erode Sengunthar Engg college,Anna University, Indiay, E-mail-cbalu.cse@gmail.com*

Trust[1] is “the degree of realiability “of other nodes performing actions and can be formed by maintaining a record of the transactions with other nodes directly as well as indirectly. From the record a trust value will be established. Trust management system for wireless networks is a mechanism that can be used to support the decision-making process of the networks [1].It aids the members of Wireless sensor networks (trustors) to deal with uncertainty about the future actions of another participants (trusters).

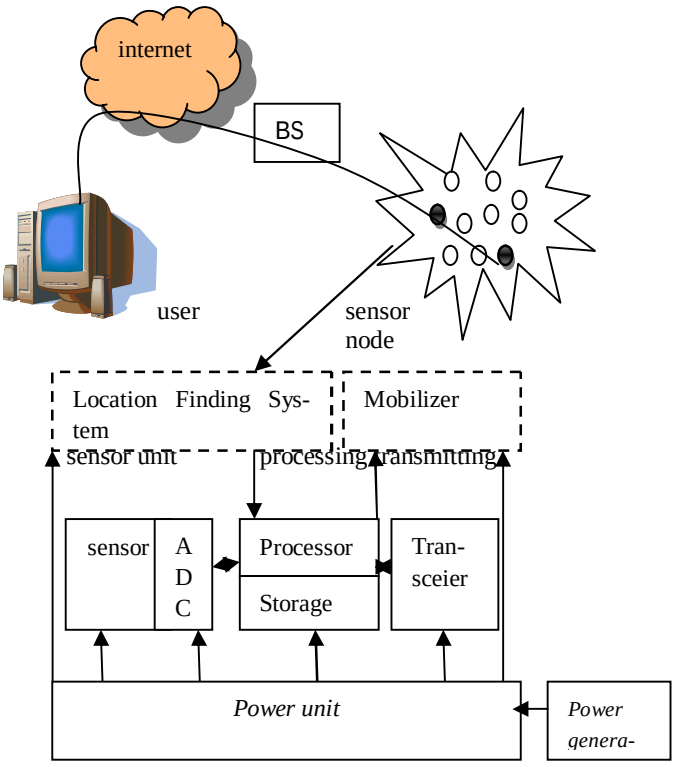


Fig 1. The components of a sensor node

A WSN is usually composed of hundreds of sensor nodes. These sensor nodes often deployed in a sensor field and have the capability to collect data and route data back to a base station (BS). A sensor consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit [1]. It may also have a additional application-dependent components such as a location finding system, power generator, and mobilize (Fig 1). Sensing units are usually composed of two subunits: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes.A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g a single battery) or may be supported by power scavenging devices (e.g, solar cells). Most of the sensor network routing techniques and sensing task require knowledge of location, which is provided by a location finding system finally a mobilizer may sometimes be needed to move the sensor node, depending on the application.

Many researchers on trust related in WSNs are processed, but it is required to design and develop a light weight trust management system that takes the less resources of the node in evolution and management of trust between/among the nodes. The trust management of the wireless sensor networks should be as simple as possible.

The paper organized as follows section2 describe the related works on trust based routing model, section 3 presents the problem description , and section 4 presents the overview of the trust aware routing protocol among the nodes and the trustworthy from source to BS. And section5 describe the conclusion of this paper.

2 RELATED WORK

Recently, There have been significant research works on security mechanism used in WSNs. This section covers the literature survey of the work of the paper.

In [2], the authors have carried out a survey of protocols and algorithms proposed for the WSNs. They have tried to produce a better understanding of the current research issues in the emerging field of technology.

In [3], the authors provide a ARIADNE protocol. It absorbs the ideas of SPINS and came out with the a hardened version of DSR. One of the requirements is that every node has to be able to generate an one-way key chain. Since the memory of sensor node is limited, it cannot afford to generate a long key chain, and so has to spend lot of time generating keys, By enforcing authenticity alone, ariadne does not guard against attacks by multiple colluding nodes It is very efficient protocol, using a highly efficient cryptographic primitives and per-hop function. It prevent the attackers or compromised nodes from tampering.

In paper [4], the authors said ATSR (Ambient Trust Sensor Routing) protocol. It is a fully distributed management system is realized in ATSR in order to evaluate the reliability of the nodes. Using this approach nodes monitor the behaviour of their neighbours in respect to different trust metrics and finds direct trust value per neighbour.

In [5], the author defined Trusted AODV protocol ,it is extended AODV routing protocol to perform routing by taking trust metrics into account .First a trust recommendation mechanism is introduced and then the routing decision rules of ADOV are modified to take trust into account.

Authors In [6], presented a Trusted GPSR .The Greedy Perimeter Stateless Routing is modified to take trust levels of node in to account .Each time a node sends out a packet it waits until it overhears its neighbouring node forwarding it. Based on this correct and prompt forwarding information it maintains a rust value for its neighbours .This information is then taken into account in the routing decisions.

In paper [7] ,the authors designed the SPINS protocols. It mainly composed of two building blocks(1) SNEP(secure network encryption protocol) is used to provide data confidentiality, two-party authentication and data freshness (2)µTELSA(Micro version of Timed, Efficient, Streaming , Loss-tolerant Authentication protocol) this provides authenticated streaming broadcast. SNEP provides its features by semantic encryption; however, we can notice that these security services do not have a provision for secure routing. In other words, SNEP is an end to end security protocol and cannot prevent routing misbehaviour. On the other hand, µTESLA provides a secure broadcast communication, which is a common and important communication pattern in almost all WSNs applications.

In Paper [8], the authors said the Trust-aware DSR protocol The watchdog and pathrater modules has been designed and incorporated in the Dynamic Source Routing protocol. The watchdog protocol is monitoring part that is designed to be responsible for detecting only non forwarding misbehaviour. This is accomplished by overhearing the transmission of the next node. The node thus is assumed to be in a continuous promiscuous mode. When the attack is detected, the observing node informs the source of the concerned path. In this approach, each node maintains a buffer of recently send packets. In case the packet is not forwarded on with in timeout or overhead packet is different than the on stored in the buffer, the watchdog increments a failure counter for the node responsible for forwarding the packet. If the counter exceeds a certain threshold, the node is considered as misbehaving and

the source is notified.

The pathrater is the component used for reputation Ratings are kept about every node in the network based on its routing activity and they are updated periodically. Node select routes with the highest average node rating. Thus, nodes can avoid misbehaving nodes in their routes as a response. The pathrater combines knowledge of misbehaving nodes with link reliability data to select the route most likely to be reliable. Specifically, each node maintains a rating for every other node it knows about in the network and calculates a path metric by averaging the node ratings in the path, enabling thus the selection of the shortest path in case reliability information is unavailable.

Negative path values indicate the existence of one or more misbehaving nodes in the path. If a node is marked as misbehaving due to temporary malfunction or incorrect accusation, a second –chance mechanism is considered, by slowly increasing the ratings of nodes that have negative values or setting them to anon-negative values after a long-timeout. However, misbehaving nodes still transmit their packets as there is no punishment mechanism adopted here. Moreover, no second hand information propagation view is considered which limits the cooperativeness among nodes.

In [9], the authors introduce a CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks).A routing protocol for MANET with predetermined trust, and later improved it with an adaptive Bayesian reputation and trust system and an enhanced passive acknowledge mechanism(PACK). It is a reputation based secure routing framework in which nodes monitor their neighbourhood and detect different kinds of misbehaviour by means of an enhanced PACK mechanism.

The nodes use the second-hand information from others as a resource of rating, as well. The protocol is based on Bayesian estimation that aims to classify other nodes as misbehaving pr normal. The observing node excludes misbehaving nodes from the network as a response, by both avoiding them for routing and denying them cooperation. In this approach, Upon detection of the nodes malice, its packet are not forwarded by normally behaving nodes, while it is avoided in case of a routing decision and deleted from a path cache. CONFIDANT architecture compromises 4 components residing on each node: the monitor, the reputation System, the Path manager and the trust manager components.

The monitor component enables nodes to detect deviations of the next node on the source route by either listening to the transmission of the next node("passive acknowledge") or by observing route protocol behaviour. In order to convey warning information in case of identification of a bad behaviour, an ALARM message is sent to the Trust Manager component, where the source of the message is evaluated.

The rating is updated only if there is sufficient for a node and that has occurred a number of times, exceeding a threshold to rule out coincidences. Evidence could come either from a nodes own experiences through the monitor system or from the trust manager in the form of Alarm messages. Second-hand information is attributed with low significance with respect to the first-hand information, irrespective of its source node. Local rating lists and/or black lists are maintained at each node and potentially exchanged with friends. Black lists may be used in a route request, so as to avoid bad nodes along the way to the destination or to not handle a request originating from a malicious node and in forward packet request, so as to avoid forwarding packets for nodes that have bad rating. The protocol assumes a Dynamic Source Routing (DSR) operational routing protocol and lacks a provision on WSN constraints and conditions as it designed for general ad-hoc networks.

In paper [10], the authors said TRANS protocol. TRANS (Trust Routing for Location Aware Sensor networks) is a geographic routing protocol(GPSR-based) that provides security services using trust metric. It can be considered as a tight trust-based routing due to its specific targets and assumptions. It basically targets a misbehaviour model in which an attacker selectively participates in routing signalling and control packet but drops consistently queries and data packets. The protocol also assumes static sensors networks in which a tight mapping can be done between the nodes identities and their locations. TRANS assumes a location-centric architecture that helps it in isolating misbehaviour and establishing trust routing in sensor networks. As a result of that, the protocol assumes that certain communication model in which a single or multiple sinks initiate communication requests with various locations.

During the phase, insecure locations are identified and blacklisted. The trust metric used to judge on location security is calculate based on nodes experience among each other regarding their identities, link availability and packet forwarding.

In paper [11], the author proposed a distributed trust-based framework and a mechanism for the selection of trustworthy cluster heads in a cluster- based wireless sensor networks. The model uses direct and indirect information coming from trusted nodes. Trust is modelled using the traditional weighting mechanism of the parameters: packet drop rate, data packet and control packets. Each node stores a trust table for all the surrounding nodes and these values are reported to the cluster head only and upon request. This approach is not based on the second-hand information, so it reduces the effect of bad-mouthing.

In paper [12] ,the author describe SAR(Security – Aware Routing) protocol derived from ADOV and based on

authentication and a metric called the hierarchical trust value metric. The hierarchal trust values metric governs routing protocol behaviour. This metrics is embedded into control packets to reflect the minimum trust value required by the sender. Thus, a node that receives any packet can neither process it nor forward it unless it provides the required trust level presented in the packet. Moreover, this metrics is also used as a criterion to select routes when many routes satisfying the required trust value are available.

The work in [13], is RGR (Resilient Geographic Routing) protocol is also a trust-based routing protocol that relies on a modified routing operation on GPRS. The basic idea in RGR is to assign an initial trust value for each node. Then, this value is incremented or decremented depending on the forwarding activity of the monitored node using a step function. The source node selects probabilistically a subset among its neighbours to forward its packet. This subset is selected from the nodes forwarding set that exhibits trust
Values greater than a threshold.

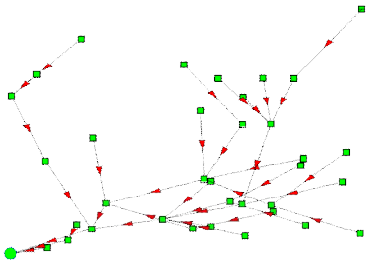
Based on the literature surveyed above, the challenges of WSNs such as keeping the hop-by-hop flow control method for data transmission, energy management.

3. PROBLEM DESCRIPTION

There are many new routing protocols proposed for WSNs , unfortunately security issues arise with these protocols, because security features are not designed built-in. So following problems in WSNs

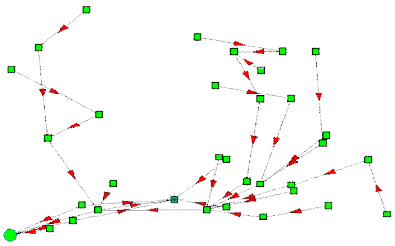
(1)Secure Route Discovery: Assume that the initiator A performs a route discovery the for target B, and that they share the secret keys KAB and KBA respectively, for message authentication in each direction. Route discovery mechanism should enable the target to verify the authenticity of the route requestor, it also need to authenticate data in route request messages and route messages through the using of KAB and KBA. Malicious nodes may avoided during route discovery.

(a) Normal Scenario



Base Station
Node

(b) A fake BS Attracts traffic



BS Node Fake Base Station

(2) Route Maintenance: A node forwarding a packet to the next hop the source route returns a route error message to the original sender of thePacket if it is unable to deliver the packet to the next hop after a limited number of retransmission attempts. It is a big issue to secure those route error message and prevent unauthorized nodes from sending those messages.

4. PROPOSED SYSTEM

A TRUST AWARE ROUTING OVERVIEW

In this section, an overview of the proposed trust aware system will be presented.

4.1 Trust aware routing

4.1.1 Definition

A trust aware routing protocol is a routing protocol in which a node incorporates in the routing decision its opinion about the behaviour of a candidate router. This opinion is quantified and called trust metric. Trust metric should reflect how much a router is expected to behave, for example, forward a packet when it receives it from a previous node.

Obtaining the trust metric is a problem by itself since it requires several operational tasks on observing nodes behaviour, exchanging nodes experience as well as modelling the acquired observations and exchanged knowledge to reflect nodes trust values .

4.1.2 Importance

Trust aware routing in WSN is important for both securing obtained information as well as protecting the net-

work performance from degradation and network resources from un reasonable consumption

. Most WSN applications carry and deliver very critical and secret information like military and health application. A WSN network infected by misbehaving nodes can misroute packets to wrong destinations leading to misinformation or do not forward packets to their destination leading to loss information .Such application can be very sensitive to these attacks. Having a trust aware routing protocol can protect data exchange, secure information delivery and maintain and protect the value of the communicated information.

Node misbehaviour can cause performance degradation as well. For example, non forwarding attacks decrease the system throughput since packets will be retransmitted many times and they are not delivered. An infected WSN network can be partitioned into different parts that cannot communicate among each other due to non forwarding attacks. This leads to the demand increasing the number of sensors or changing the node deployment to the demand of increasing the number of sensors changing the node deployment to return network connectivity. This is very expensive however,can be avoided if a good secure routing solution is adopted.

A trust aware routing framework for WSNs called sTARF to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information. This approach identifies malicious nodes that misuse “stolen” identities to misdirect packets by their low trustworthiness, thus helping nodes circumvent those attackers in their routing paths. It incorporates the trustworthiness of nodes into routing decisions allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. It significantly reduces negative impacts from these attackers.

Our system is fully distributed in the sense that each node implements all modules with the full functionality.

4.1.3 A Node and Trust relationship

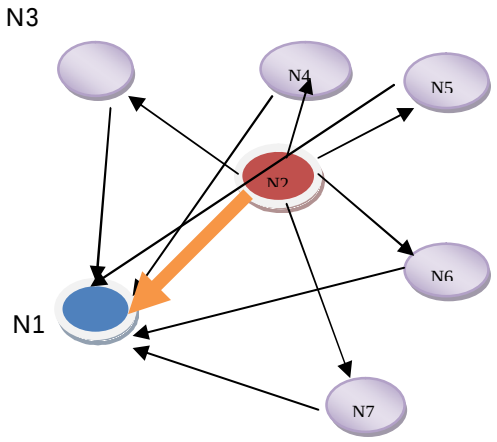


Fig 2: A node and Trust relationship

Node N1 wants to find the trust on N2

Node N2 neighbours are N3,N4,N5,N6 and N7

1. The solid arrow indicates the information about the node N2 given its neighbour node to N1
2. The dark arrow indicate the direct experience.[12]

Some notations are used that are,

Notations used in proposed system

Node	N
Trust level	T
Energy cost	E_N
Average Energy cost	$E_{N\rightarrow b}$
Unit sized data packet	E_{unit}

Table 1

In this approach, to route a data packet base station, a node only needs to decide to which neighbouring node it should forward the data packet considering both the trustworthiness and the energy efficiency. It maintains a neighbourhood table with trust level and energy cost values for certain known neighbours. Two types of routing information that need t be exchanged in addition to data packet transmission are

(i)Broadcast messages from the base station about data delivery and,

(ii)Energy cost report messages from each node. Neither message needs acknowledgement.

A broadcast message from the station is flooded to the whole network. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbours once. Any node receiving such an energy cost report message will not forward it.

In this each node have two module . Energy Watcher and Trust Manager running on it in order to maintain a neighbourhood table with trust level values and energy cost values for certain known Neighbours.

ALGORITHM FOR NODE SELECTION

Step 1: Start

Step 2: The source node send out request to the Neighbour node and returns the trust. level of the respond cooperation node.

Step 3: Find the energy cost of the each node.

Step 4: Compare the trust level values with the

neighbourhood table values.

Step 5: Traverse the neighbourhood table for an optimal candidate for the next-hop.

Step 6: Decide whether to switch from the current candidate to next-hop candidate.

Step 7: stop

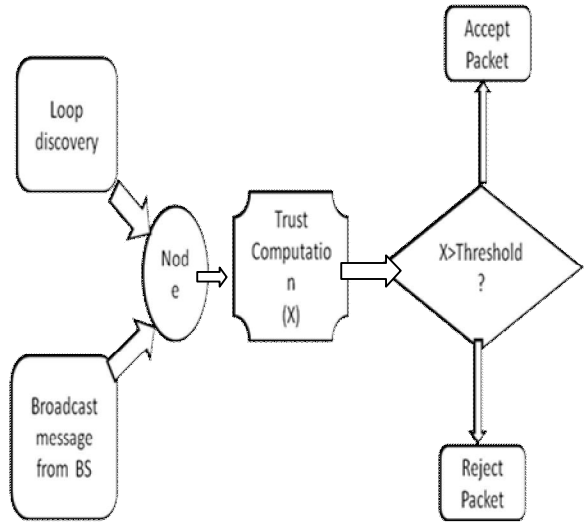


Fig 3 System Architecture

a)Energy Watcher is responsible for recording the energy cost for each known neighbour, based on nodes observation of one-hop transmission to reach its neighbours and the energy cost report from those neighbours . A compromised node may falsely report an extremely low energy cost to its neighbours intoselecting this compromised node as their next-hop node; however, these enabled neibours eventually abandon that compromised next hop node based on its low trustworthiness as tracked by Trust Manager.

b)Trust Manager is responsible for tracking trust level values of neighbours based on loop discovery and broadcast messages from the base station about data delivery. At the beginning, each neighbour is given neutral trust level. After any of those events occurs, the relevant neighbours trust levels are updated.

Occurrence of a loop degrades that nodes next-hop nodes trust level are there may be gradually taking the trust level to a low value leading to the breaking of the loop by changing its next-hop selection. On the other hand , to detect the traffic misdirection by nodes exploiting the replay of routing information.

Trust Manager computes the ratio of the number of successfully delivered data packets which are forwarded by this node to the number of those forwarded data packets, denoted as delivery Ratio.

Once a node is able to decide its next hop neighbour according to its neighbourhood table, it sends out its energy report message. It broadcast to all its energy cost to deliver a packet from the node to the base station.

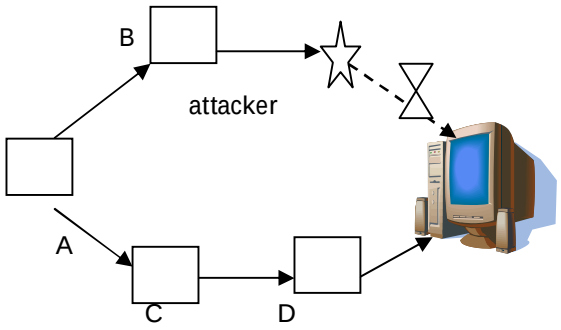


Fig 4 Working model of trust manager

Fig3 given the example to working model of trust manager, in this A,B,C and D are all honest nodes and it does not compromised. Node A has a node B as its current next-hop node while B has an attacker node as its next-hop node. The attacker drops every packet received and thus any data packet passed to node A will not arrive at the BS. After A while, node A discovers that the data packets forwarded did not delivered.

The trust manager on node A starts to degrade the trust value level of its current next-hop node B although node B is absolutely honest. Once the trust level becomes too low, node A decides to select node C as its next-hop node. In this way A identified a better and successful route
(A-C-D-BS).

CONCLUSIONS

In this paper we have presented a survey of the routing protocol that specifies how it provide better routing path for transmitting the packets from source from destination. And we presented a over view of Trust aware routing protocol for secure routing in Wireless sensor Networks, and modules involved in that to improve the performance , Finally we design how the modules are selecting the better route for transmitting packets.

REFFERENCES:

[1] M. Momani, "Bayesian Methods for Modeling and Management of Trust in
Wireless Sensor Networks," Ph.D.Thesis, University of Technology,

Sydney, July, 2008.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine,40(8):102–114, August 2002.

[3] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Net works", Proc. Eighth Ann. Int'l Conf. Mobile Computing and Networking (MobiCom), pp. 12-23.

[4] Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Voliotis, "Mobile Net works Trust Management in Wireless Sensor Networks", European Transactions on Telecommunications, 2010; 21:386-395.

[5] Xiaoqi Li, Ly u, M.R., Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad-hoc Networks", IEEE Proceedings on Aerospace Conference, 2004, vol. 2.

[6] Asad Amir Pirz ada and Chris M cDonald, "Trusted Greedy Perimeter Stateless Routing", IEEE, ICON 2007.

.

[7] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, " SPINS: Securit y Protocols for Sensor Networks", ACM Journal of Wireless Net works, 8:5, September 2002, pp. 521 – 534.

[8] S. Mart i, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad-hoc Net works", in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), ACMPress, 2000, pp. 255 – 265.

[9] S. Buchegger and J. Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness In Distributed Ad-hoc Networks", in proceedings of the 3 ACM International Symposium on Mobile Ad-hoc Networking and Computing (MobiHoc), ACM Press, 2002,
pp. 226-236.

[10] Sapon Tanachaiwiwat, Pinalkumar Dave, RohanBhindwale, Ahmed Helmy , "Location-centric Isolation of Misbehavior and Trust routing in Energy-constrained Sensor Net works", IEEE International Conference on Performance, Computing and communications, 2004.

[11] G. V. Crosby, N. Pissinou and J. Gadze, "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks", in The Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06), Columbia, Maryland, 2006.

[12] S. Yi, R Naldurg, and R. Kravets, "Security-aware Ad-hoc Routing for Wireless
Networks", ACM Wksp. Mobile Ad Hoc Networks, Mobihoc, 2001.

[13] Nael AbuGhazaleh, Kyoung Don Kang and Ke Liu. "Towards Resilient Geographic
Routing in WSNs", MSWiM'05, October 10–13, 2005.