JEAS | Journal of Economics and Administrative Sciences
E-ISSN: 2148-1792 P- ISSN: 1302-2024
Volume 4, Supplement Issue 1
www.jeasweb.org

Studying Trust-based Routing Protocols in Wireless Sensor Networks

Samira Tabandeh
Master of Computer Software Orientation, Islamic Azad University, Kerman, Iran.

Farokh Koroupi
Head of computer department, Ph.D. from Birmingham university of England, Birmingham, England.
Assistant Professor, Azad University of Baft, Baft, Iran.

ABSTRACT

Wireless sensor network (WSN) is a special kind of Ad Hoc Networks and involves a set of small nodes that can sense the surrounding environment with a specific purpose, information processing, storage, exchange of information with other nodes, as well as the ability to adapt to changes (topology, and so on). Usually all nodes are the same and in practice work together to reach the overall goal of the network. The purpose of WSNs is to monitor and control the conditions and atmospheric, physical or chemical changes in an environment with a definite range. By expressing the basics of WSNs, the study examined different types of trust-based routing protocols.
Keywords: wireless sensor network, routing, protocol, trust

Introduction

The history of sensor networks dates back to the Cold War (mid-1950s) and Sound Surveillance System (SOSUS) (Nishimura et al., 1993). The first examples of sensor networks had been designed and implemented for military applications so that military forces could communicate in a new area with no need to set up special equipment related to network infrastructure.

The process of using sensor networks continued in the late 1980s and early 1990s by Defense Advanced Research Projects Agency (DARPA) and some other countries, and research groups at the universities were carrying out some innovations. In the mid-1990s, with the definition of some standards like Engineers Institute of Electrical and Electronics (IEEE) 1999, commercial technologies started to emerge as well, and various research groups active in the field of wireless communications entered the potentially large-scale civilian market. Indeed, the samples commercially used now are the result of the efforts made in the research environments of the early years.

In WSNs, a large number of nodes with facilities like broadcasting, processing, sensing, and so on are scattered in a specific frame environment. The happened events, or the questions asked by sink and the mission assigned to each node lead to connections between the nodes. The information exchanged can be a report of the status of the area under the control of the sensor nodes to the sink or a request from the sink to the sensor nodes. As the communication port of the sensor network with other telecommunication systems and networks, sink is the final recipient of the report from the sensor nodes and after performing a series of processes, it sends the processed information to the user (using a communication medium like

the Internet, satellite, and so on). On the other hand, user requests are transmitted to the network by this node.

The essence of sensor networks is that what they do must be local, as each node can only communicate with its neighbors, and the general and global information from the network is not that available (Gathering this information needs a lot of cost and time). The information obtained by the nodes must be sent to sink in some way using routing techniques.

Establishing and designing the structure and architecture of communication between network nodes needs observing different factors like fault tolerance, scalability, production cost, operating environment, sensor network topology, hardware limitations, communication tools and media, energy consumption, and so on.

Factors like the economics of the system, the expected capabilities, mass of nodes, and the practicality of the ideas in the real environment have made each node face some hardware limitations (Ilyas et al., 2004).

WSNs are intended for statistical observation as well as tracking one or more specific targets in the environment. Given the inherent characteristics of sensor networks, they can be used in different applications. Considering all the characteristics, sensor networks have a high capacity besides low consumption costs in the field of environmental monitoring. The small size of the sensor nodes and the ability to be located in every corner of the information acquisition in detail, lack of harmful environmental impacts, data storage in the event of an accident, and non-interference with other telecommunications systems can be good reasons to justify the use of sensor networks over other similar systems in such surveillance uses.

Protocol stack

According to Figure 1, the protocol stack of sensor networks on the one hand has five layers like physical layers, link and Medium Access Control (MAC), network, transmission and application and on the other hand has three phases of energy management, motion management and task management (Akyildiz et al 2002). The task of the physical layer is modulation, sending, and receiving at a low level. The Media Access Control Layer should be able to communicate with any neighboring node with minimum collision using broad casting. The network layer is responsible for routing. The transfer layer is responsible for managing the transfer of packets if needed. Depending on what the network is designed for, various types of application software can be used on the application layer and present various services.

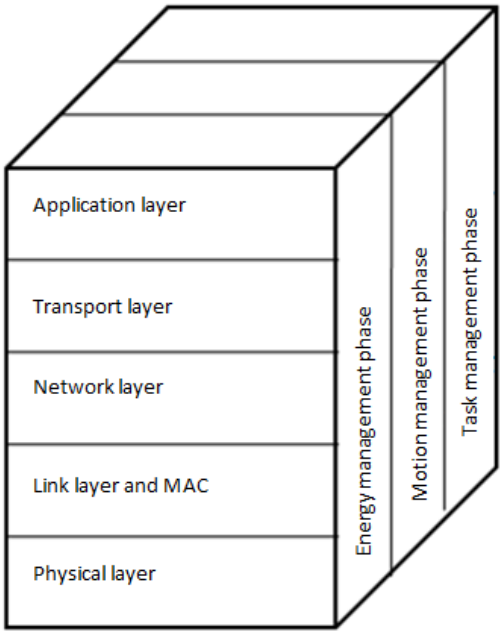

Fig. 1: Protocol stack of sensor networks

Goldsmith et al. (2002) has suggested another protocol stack called cross-layer protocol stack for sensor networks (Figure 2). In this protocol stack, the boundary between the different layers is very loose and the layers are developed in a hierarchical and integrated framework. This loosening of the boundary of the layers is because of the limitations and specific applications of sensor networks, which makes it possible to provide optimal and appropriate solutions and protocols for sensor networks.

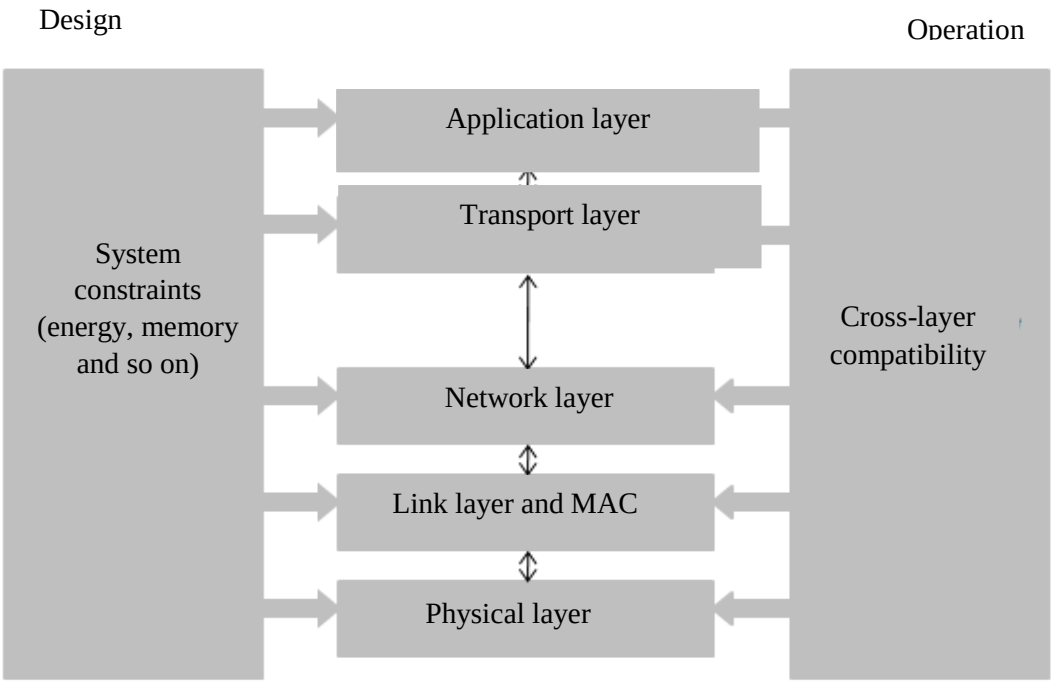

Fig. 2: Layer-cross-sectional protocol stack in WSNs (Goldsmith et al., 2002)

The following are some of the cases that should be considered while designing a communication protocol for sensor networks (Ilyas et al. 2004):

• By drop in the nodes energy, and possibly not performing the activities properly by the nodes whose energy has been consumed too much, the accuracy of the protocol performance should not be lost.

• Given the random nature of scattering of the nodes at the periphery level, the protocol should be able to apply to any randomized topology, regardless of any conditions for the nodes to be located.

• It must consider the not-so-high processing capacity of the nodes and do not consider complex and heavy processing for them.

• It must not use direct routes to transmit information as much as possible, but reduce transmission costs by passing them through intermediate nodes as transmitting a packet of information to close neighbors will consume far less energy than sending it directly to nodes that are farther away.

• It must be resistant to changes in the network because of the death of some nodes and still direct packets from other routes to the destination.

• It must have the ability to expand. In other words, with increase in the number of nodes and dimensions of the network, the cost of operations required for routing in it must increase in a limited and controlled way.

• It must not consider the existence of specific hardware in the nodes. Given the small size of each node, the existence of large-scale hardware in them is not very desirable and therefore the protocol must consider these hardware limitations.

• It must consider the problems that generally affect wireless communication.

• It must not have too much control overhead. Excessive overhead only leads to more energy consumption, so the protocol should pay attention to this issue.
• Although the quality of the service (QoS) is of secondary significance in most sensor networks, this category must be considered in its design if the application for which the protocol is provided requires QoS.

Routing protocols in WSNs

According to the existing standards, routing is done in the network layer and all the techniques and algorithms used should be the best route for transferring information packages according to the limitations and conditions in the network and according to the considered criteria and parameters from origin to destination. Because of the differences between WSN and other wireless networks, many new protocols have been proposed to address the routing problem. Sensor network routing protocols are classified into multi-routing-based, QoS-based, negotiation-based, query-based, and coherence-based routing protocols in terms of receiving environmental responses (Al-Karaki et al. 2004). Routing protocols are divided into three categories - reactive, proactive, and combined protocols - in terms of how the origin finds its way to the destination. One of the best classifications of sensor network routing protocols is the classification provided by Akkaya Younis (Akkaya et al., 2005). This classification classifies routing protocols into four general categories considering the node performance, information available to each node, and network goals: "data-driven", hierarchical, "position-based", Aware of QoS, and network flow. Some routing protocols fall into more than one category of this classification as they pursue various goals and have their own presuppositions. To determine which protocol belongs to which category, they consider the most important factor of that protocol, and considering what the emphasis of the protocol is on it, they link it to the desired category.

Data-driven routing protocols

In many sensor networks applications, assigning a public identifier to nodes is impossible. This makes it difficult for different respondents to select a particular set. Thus, data is transferred from each node to a wide range of nodes, which involves large redundancy and reduces the efficiency in terms of energy consumption. Under these conditions, routing protocols capable of selecting a specific set of nodes have been presented. These data-driven routing protocols are different from traditional address-based routing. In data-driven routing, sink usually sends its queries to specific areas and waits for the data to be taken from the nodes in that area. After the answer to the question is obtained, the answer is sent inside the data packet to sink. The first two simple and very simple algorithms for routing sensor networks are flooding and gossiping distribution (Hedetniemi et al. 1988). In flooding, each sensor receives an information packet and broadcasts it to all of its neighbors until it reaches its final destination. In gossiping, each node randomly selects one of its neighbors and sends it to it by receiving an information packet. Obviously, flooding has a very high overhead, reduced in the gossiping, but as the random neighbors selected in the gossiping may not be the right route to send the packet to the destination and there may be the need to re-select other neighbors accidentally, the transmission speed on the network reduces drastically.
In SPIN protocol, instead of disseminating packets of information, only meta-data about those packets is disseminated by each node (Heinzelman et al. 1999). This is done through a message called Advertise (ADV). In this case, each of the neighbors in this node decides based on the information received whether they need the information in the package. In this case, only the neighbors who declare their need for the packet (via request (REQ) message) will receive the complete information package. Figure 3 shows the steps of SPIN algorithm.

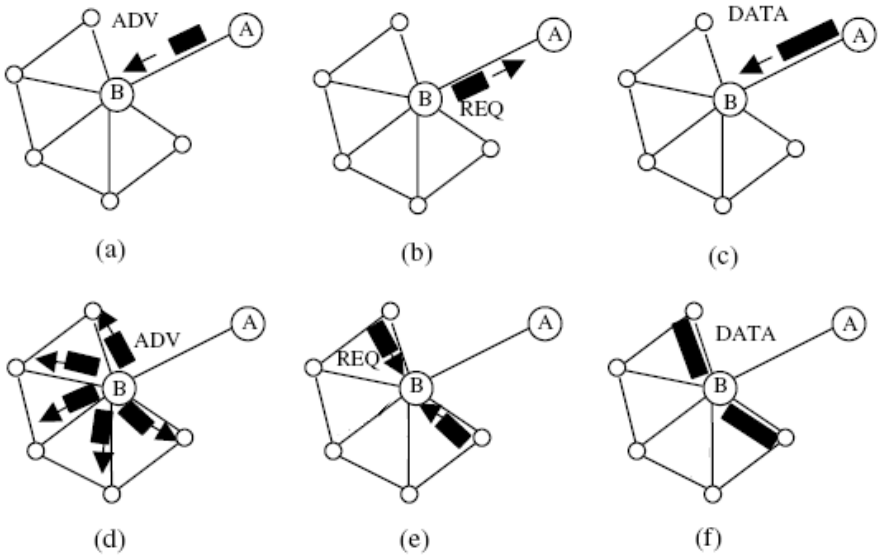

Fig. 3: Steps of SPIN algorithm (Heinzelman et al. 1999 a)

EAR Routing Protocol is one of the most important energy-aware routing protocols on sensor networks (Shah et al., 2002). EAR uses local request and broadcast messages to obtain all possible routes to the destination, placing these routes in the node routing table. Each node assigns a probability to each of its routes, depending on the energy consumed and the distance of the next node (in the desired route). In sending data by a node, that node selects a route based on the probabilities assigned to the routes and directs the data packet through that route to the destination node. By doing so, instead of using a specific route to send data packets, multiple routes are used for sending, thereby increasing the lifespan of the network.

Hierarchical routing protocols

In hierarchical routing, nodes are divided into logical clusters. In each cluster, some nodes are considered red and the other nodes are considered as members of the cluster. Cluster members obtain the desired information from the environment according to the application and then send this information to the cluster head. By collecting this information, cluster head sends it to the sink. Most hierarchical protocols have two steps to routing. The first stage is cluster head selection and the second stage is the routing. Hierarchical routing is an effective way to reduce the number of messages sent to main stations and thus increase the lifespan of the network.

One of the first and most famous hierarchical protocols for sensor networks is LEACH protocol (Heinzelman et al. 2002).

AIMRP protocol assumes that sink is located in the center of the sensor network and that the other nodes are around this node (Kulkarni et al. 2006). The protocol has two phases of configuration and activation. In the configuration stage, sink determines the nodes in the first row by sending a Tier message within the broadcast radius a. These nodes also determine the nodes in the second row by broadcasting the Tier message in the radius a. This algorithm continues until all nodes in the network determine their order. In the activation phase, each node tries to send its information, first by sending an ad, trying to find a node close to its lower row (closer to sink). After such a node is identified, a data packet is sent to it. The proposed protocol has tried to address as much as possible the problems of media access control, and to reduce the risk of collisions as much as possible by sending random delays to send information from each node. HEED has developed an algorithm for clustering node sensor nodes, where 4 goals are tried to reach: increasing the network lifespan, completing the clustering phase after a certain number of iterations, minimizing control overhead, and distributing clusters appropriately across the network (Younis et al., 2004). In this protocol, each probable node (CHprob) decides according to its residual

energy to be cluster head. This decision is temporary at first and will be finalized after several iterations. The nodes that have chosen themselves as cluster head (CH) express this to their neighbors. Each of the neighbors becomes a member of this cluster if it has not already been a member. If a neighbor is previously a member of another cluster, whose CH current residual energy is lower than the residual energy of the new CH, the neighbor joins the new CH. In addition, if the neighbor is CH, after comparing its own residual energy with that of the proposed CH, it will decide whether to stay CH or move to the new cluster. Any CH not having decided to join another cluster doubles its CHprob value and re-introduces itself as CH to its neighbors. If CHprob value in a node is greater than 1, that node chooses itself as the final CH. In this case, the neighbors of this node will also become members of the final clusters and there will be no changes. At the end of this phase, if a node has not received any cluster introduction message, it decides for itself to be a new CH.

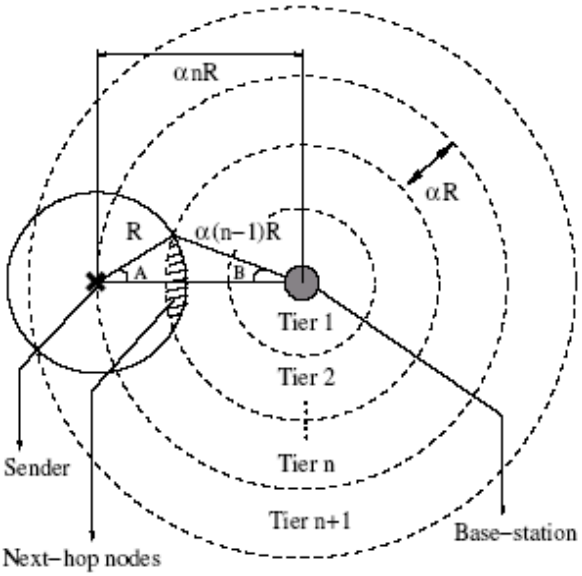

Fig. 4: Forming categories around sink for the protocol (Kulkarni et al 2006) AIMRP

Hierarchical protocols use a variety of methods to prevent interference from a cluster member's relationship with their CH. AIMRP uses a similar method to that of IEEE 802.11. However, the mechanism commonly used to link cluster members to CH is Time-Division Multiple-Access (TDMA), used in many protocols (Heinzelman et al. 2002).

Location-based routing protocols

Most routing protocols need to have information nodes of their location. In most cases, position information is needed to calculate the distance between two specific nodes to estimate energy consumption. Using the position information, one can propose effective routing solutions that save energy efficiently. For example, if the area of the sensing area is known using the position of the sensors, the questions can be extended only to that particular area, which can eliminate the number of transfers. Awareness of the position can be gained through physical devices like Global Position System (GPS) (Bulusu et al., 2000) or topology exploration algorithms (Moore et al., 2004).

PGR protocol is a protocol that uses the position and energy information of nodes to create the appropriate route to the destination (Roosta et al., 2005). In PGR, each node is assumed to know the destination. Neighboring nodes first exchange information with each other, through which each list of neighbors obtains their location and communication power. To send information to the destination, the origin node determines the list of neighbors that are at θ angle to it and the destination. After these neighbors have been identified based on the energy and the ability of the nodes, each of the nodes is assigned a probability. Then source node selects a node to send the data packet based on the probabilities

attributed. The selected node selects the next neighbor accordingly, and this process continues until it reaches its final destination. In GAF routing protocol (Xu et al., 2001), a virtual grid with square shaped cells is assumed to be on the network (Figure 5). Each node, depending on its spatial location obtained through GPS, determines which cell in the grid it is. Obviously, some nodes will be obtained for each cell in the grid. Of the nodes in each cell, only one node is active and the other nodes are inactive. After a certain period, the active node becomes inactive and one of the inactive nodes is activated. The active node is responsible for viewing the intracellular environment and participating in the routing. In the main GAF protocol, each node can only communicate with the active nodes of adjacent cells that are horizontally or vertically adjacent to the target cell. In this case, it is necessary that the length of each side of the cell be $\frac{R}{\sqrt{5}}$ according to the transmission range of each node (R). For the node to be able to communicate with the active nodes of the cells that are diametrically adjacent to the target cell, it is necessary that the length of the cell side be $\frac{R}{\sqrt{8}}$. Many protocols use the virtual grid concept presented in GAF protocol and integrate their proposed mechanism with GAF protocol (Salzmann et al., 2007). Recently, the use of 6-sided grids has been proposed for GAF protocol. This proposal only addresses the possibility of using diagonal connections using 6-sided cells (Liu et al., 2007).

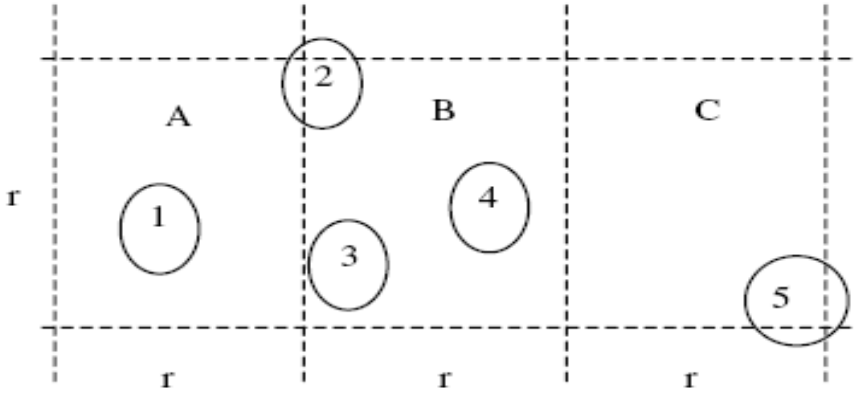

Fig. 5: Virtual grid on the sensor network, node 1 is assigned to part A, nodes 2, 3 and 4 are assigned to part B and node 5 to part C (Xu et al., 2001)

In the protocol presented by Akl and Sawant on the node distribution range, the virtual grid is considered with square cells (Akl et al., 2007). Each node of each cell can communicate with the nodes of adjacent cells horizontally, vertically, and diagonally. In each cell, the node with the larger number is active and the other nodes are inactive. By the general broadcast that the sink does, the route is created towards sink and the information is transferred from the source node to sink. Whenever the active cell node of the cell is out of energy, the node with a larger number in that cell is replaced. Virtual grid has also been used for hierarchical and clustering routing protocols (Zhang, 2006). In these protocols, a network of virtual grids with square cells is considered as the CH selected from among the nodes within each cell. The selected node has the ability to communicate with CHs of neighboring cells or sink.

QoS and network flow aware routing protocols

Although most of the proposed routing protocols for sensor networks fall into the previous categories, some algorithms have considered other factors like QoS and network flow. QoS aware protocols examine end-to-end delay, network lifespan, and so on. Protocols like "data collection with maximum lifespan", "Minimum Cost Forwarding (MCF)", Sequential Assignment Routing (SAR), and so on are in this category. Some of these protocols are described below.

MCF protocol is based on the three cost factors of link delay, throughput, and the node residual energy (Ye et al., 2001). The proposed algorithm has two phases. In the first phase, sink releases the Interest

packet at the network level. By receiving Interest, each node calculates its cost based on the cost received from the previous node and the cost of the communication link, and sends the packet to its neighbors at a new cost. Thus, at the end of this phase, all nodes will determine their communication cost to sink. The second phase involves the transfer of packets to sink. In this phase, the node with a packet to send sends its communication cost to sink at the top of the packet and publishes the packet to its neighbors. Each neighboring node checks the cost of the packet header. If the neighbor's communication cost is higher than sink, it will remove the packet without any operations. However, if the cost of communication to sink is less than the cost of the packet header, it first changes the packet header to include its communication cost to sink, and then broadcasts the packet to its neighbors.
SAR protocol has trees whose roots can be directly related to sink (Sohrabi, 2000). The edges of this tree are determined by considering three factors: QoS, energy resources in each route, and the priority level of each packet. Thus, multiple routes will be obtained from sink to each of the sensors. While sending information, one of these routes is selected based on QoS and resources available on each route.

Trust-management in WSNs

In an environment without infrastructure sensor networks, nodes rely on partnership to navigate and send their packets to the base station. Many attacks specifically target routing processes. An approach taken from human societies has been proposed to counter these attacks. In those nodes, they monitor the behavior of their neighbors to assess their reliability according to the specific behavioral aspects called Trust Metrics. Based on these, nodes build trust relationships among themselves and make their routing decisions not just based geographic information or other poor routing information, but based on their predictions of the sincere participation of all neighbors (or their trust in them), according to which a trust management system is implemented. Although key-based methods can be used to maintain data accuracy, encryption and powerful methods are authentication of powerful tools to protect packet integrity and node validity, they cannot detect a large set of routing attacks, such as selfish behaviors, selective sending, black holes, slander attacks, and so on. Thus, a trust model more is used for higher layer decisions like routing, data aggregation, as well as selecting a CH or even key distribution. Trust management methods are a powerful tool for detecting unexpected behavior of nodes (whether malicious nodes or damaged nodes). When bad behavior nodes are identified, their neighbors can use the information to prevent them from participating in data transmission, data aggregation, and other collaborative activities.

Trust-Aware Routing Framework (TARF) for WSNs

This method performs a multi-route routing in sensor networks by evaluating the reliability of neighboring nodes, identifies unreliable nodes and avoids them in routing. This approach focuses on energy efficiency and trust. The originality of this protocol focuses on attacks where a network traffic attacker misleads the identity by repeating routing information. The advantage of this method is that it does not need severe time constraints or geographic information. The protocol is implemented as a low-load module in the TinyOS operating system and can be embedded in the existing routing protocols with the least amount of software. Its goals are high throughput, energy efficiency, adaptability and scalability. One of its disadvantages is that it does not have a solution for Denial of Service (DOS) attacks and does not consider like low latency, balanced traffic load and fairness of resource distribution, so it detects the route from the beginning when it detects a fault node in the route (Jean et al., 2012).

Trust Based On-demand Distance Vector (AODV) routing protocol

This protocol is the developed form of the well-known AODV protocol, designed to perform routing based on confidence criteria. In this mechanism, first, a trust method is proposed and then AODV routing rules are changed to consider trust. The special emphasis of this method is that a set of policies is inferred for a node to update its opinion about other nodes according to them. Thus, a trust-information exchange mechanism is designed during the network routing process. The protocol specifically defines the processes of proposing trust, judging trust, providing information along with developing routing tables, developing routing messages, and discovering trust-based routes (Li et al., 2004).

Trust Based Energy Aware on AODV (TEAODV) routing protocol
This is an energy-aware trust-based routing protocol developed by adding trust to EAODV routing protocol. This protocol is very similar to Trusted AODV protocol, with the difference that it uses EAODV instead of AODV. In this protocol, two values of route trust and node trust are used. Each node for each route in its routing table calculates the route trust, and in the level of trust is that a packet can reach its destination. Node trust is calculated based on the difference between the values of the advertised trust nodes to the destination and the amount of trust observed to transfer the current data. These values are used in routing decisions then (Raymond et al. 2008).

Trust Link State Routing Protocol (TLSRP)
A new algorithm for constructing a reliable route from the source node to the well is provided by considering direct and indirect trust by Babu et al. (2011). Trust is calculated based on its n-th root of node QoS and the experiences suggested by its neighbors. This is a modified model of LSR protocol. The resistance of this method against various attacks has not been evaluated. The process of calculating the trust of two nodes is as follows:

$$TE_{i,j}\ or\ TE_{j,i} = \frac{\left(T_i(J) + T_j(I)\right)}{2}$$

Equation. 1: The relationship between two-node trust evaluations like TLSRP protocol

Ambient Trust Sensor Routing (ATSR) Protocol
It is a well-distributed algorithm for node reliability evaluation. According to this algorithm, nodes monitor the behavior of their neighbors according to specific trust criteria and calculate a certain amount of direct trust for each neighboring node. ATSR uses indirect trust too. It then combines the two values to gain total trust. Finally, it recognizes the secure nodes of the network and is only related to them for routing (Zahariadis et al., 2010).

Trust-Based Routing Framework in Energy-Constrained (TRUSTEE) Protocol
A trust-based routing method has been proposed in sensor networks with energy constraints. This method is a flexible and practical method that evaluates the quality of routes. Therefore, it selects the route that best meets the security needs. In this method, it is assumed that each node contains information about its neighbors, and to communicate securely with neighbors, they share keys through key pre-distribution methods. This method not only minimizes the consumption of resources like memory, energy and computational overhead, but can also perform well against external attacks due to the identification of nodes and is also able to defend against selective attack attacks. Thus, network traffic increases significantly (Weifang et al., 2006).

Trust Aware Dynamic Source Routing (TDSR) Protocol
A mechanism including "Watchdog" and "Routerater" modules has been used to ensure the security of the DSR routing protocol. The proposed method can be used in routing protocols where the source determines the route of the packets. Watchdog is responsible for detecting selfish nodes that do not send packets. To do this, each node in the network holds the sent packet in its buffer for a limited time. During this time, each node has its own wireless interface to determine whether the next node will send the packet. Routerater assigns different degrees to nodes based on feedback received from Watchdog. These grades are later used to select routes including nodes with the highest degree. Like TAODV, it improves security. However, it is not able to counteract all available attacks (Marti et al., 2000).

CONFIDANT trust-management based routing protocol
The proposed method adds a trust management system and a reputation mechanism to Watchdog and Routerater methods. Trust management manages events reported by Watchdog and issues warnings to notify other nodes about malicious nodes. Warning recipients are kept in a list called Friend-List, which is

configured to the user through a user authentication mechanism. The reputation mechanism keeps a blacklist in each of the nodes and shares it with the nodes in the friends list. The proposed protocol implements a punishment-based approach by not sending packets from nodes whose trust level is below a certain threshold (Pirzada et al., 2006).

CORE management-based routing protocol

This protocol is similar to CONFIDANT, except that it uses a complex reputation-exchange system. CORE divides the reputation of a node into three distinct components. Direct reputation gained through personal observations, indirect reputation that is a positive report by another node, and operational reputation based on supervised behavior during a particular job. These values of reputation are combined to achieve total reputation in a weighted state (Buchegger et al., 2002).

Trusted GPSR management-based routing protocol

In this method, GPSR algorithm has been developed to consider trust. For this purpose, each time it sends a closed node, it waits until the packet is sent by its neighbors, so the node maintains a certain amount of trust for its neighbors based on this information (fast and immediate sending), used in routing decisions (Michiardi et al., 2002).

TRANS management-based routing protocol

It is a routing protocol that selects routes from nodes based on trust information and not based on the number of steps or other criteria to avoid unsafe locations. This protocol is based on the assumption that sensors know their approximate position and uses geographic routing (e.g., GPSR). In TRANS, a trusted neighbor is the sensor able to decrypt the request and is reliable enough (given its track record of being sent by wells and other intermediate nodes) and a well sends messages only to its trusted neighbors (nodes whose trust value is greater than the threshold of trust). So do their neighbors who send packages to trusted neighbors who have the closest location to the destination. Therefore, the packets reach their destination through a series of reliable sensors. An important feature of TRANS is that creating a blacklist is distributed by the well.

This is due to the assumption that the well node is not endangered. By observing the responses, the well identifies the misbehaviors, explores the potential locations of the misbehaviors, and isolates the insecure locations. After removing large amounts of packets, the search engine starts searching for unsafe locations along the route, recording them and reporting the information to neighboring nodes (Pirzada et al., 2007).

SPINS management-based routing protocol

A set of security protocols optimized for sensor networks to create data privacy has provided two-way authentication and proof of confidentiality. However, it does not do much in connection with denial of service attacks or endangered nodes, and only ensures whether an endangered node discloses network keys (Tanachaiwiwat et al., 2004).

ADRIADNE trust-based routing protocol

A secure routing protocol is a demand on demand networks that prevents the manipulation of healthy routes, including healthy nodes, by attackers or endangered nodes, and prevents a large number of types of attacks, such as banning the service. This efficient protocol uses only high-performance symmetric encryption principles. It also uses clustering functions at every step, as well as advanced authentication mechanisms such as TESLA and MAC (Perrig et al., 2002).

Optimized Link State Routing Protocol (OLSR) protocol

The optimized routing protocol provides a link mode for case networks and sensors. This protocol operates as a routing table and falls into the category of active protocols in the category of routing protocols. Network topological information is regularly exchanged between other nodes in the network. Each node selects a set of neighbors as multi-steps. In OLSR, only the nodes selected as Multipoint

Relays (MPRs) are responsible for controlling and managing the networks exchanged flows, and are responsible for broadcast these packets throughout the network. OLSR protocol uses step-by-step routing. For instance, each node uses its local information for routing packets.
The idea of routing is simple and can be expressed in five sections, so each router must:

- Identify its neighbors and know their network addresses
- Measure delay or cost to its neighbors
- Create a packet that contains all the information obtained
- Send these packages to all routers
- Calculate the shortest route to any other router
- OLSR routing protocol also follows these rules.

OLSR protocol operation steps

1. Production of control packets
2. Sending packets to other nodes
3. Building the tree of the shortest route (via Dijkstra's algorithm)

Building routing table

• In OLSR, first MPR are identified. These are the only points on the network that allow data to be transmitted and reduce network overhead and sending control packets. The first task of OLSR is to identify its neighbors and do so by sending a Hello packet to the neighbors around each node. Thus, each node identifies the nodes around it. With the information obtained, each node creates a table for itself, and the node communications with its neighbors are in the table.
• In the next step, each node sends its information along with the sequence number in the form of a TC packet to the surrounding nodes. However, transfer TC packets are done only through MPR nodes. Thus, all nodes in the network are aware of the communications and how to communicate with each node with the relevant information stored in a table for each node.
• In the next step, each node of the collected information must select the best route to the destination node. Selecting the best route is done through Dijkstra's algorithm. After this step, each node has a routing table with the best route to the surrounding nodes. In this case, the network becomes stable. As the nodes location changes, the above operations are repeated and the tables are updated.

Table 1: Security challenges of OLSR protocol

Defense method	**Type of attack**
Using asymmetric keys	Not forwarding data to the packet
Authentication and key distribution	Attacking the node on the network
PKI and alignment algorithm	Generating the incorrect message
No solution has been proposed	Jamming attack
Using time tag	Response attack
Periodic announcement of each node concerning the packets received from its neighbor	Wormhole attack

• Producing incorrect control messages: One of the ways where a node can act incorrectly; in other words, producing control messages that are incorrect according to OLSR
Such messaging attacks are as follows:

1. Generating incorrect HELLO messages
2. Generating incorrect TC message

Generating incorrect MID / HNA messages

• Generating incorrect relaying control messages: (related to MPR selection) including the following attacks:

1. Black Hole attack
2. Response attack
3. Wormhole attack
4. MPR-Flooding attack

Conclusion

Sensor networks, which have received great attention in recent years, consist of a large number (which may reach thousands) of small, low-cost, high capability sensor nodes with low-energy storage. These sensors can receive information (like temperature, humidity, pressure, and so on) from their surroundings and send it to neighboring sensors. Sensor network has proposed a new control and surveillance model that has various applications in scientific and non-scientific areas like environmental, military, transportation, medicine, and so on monitoring. Given the constraints of sensor networks, it is necessary to provide new techniques for various problems in them. Among the problems raised in sensor-networks are routing, fault tolerance and topology control. The routing problem in sensor networks has received many efforts in recent years and has introduced unique challenges compared to traditional routing in wired networks. Routing protocols are used to facilitate communication within the network and to cover routes between nodes. One of the most complete classifications of routing protocols divides routing protocols into four general categories: data-driven, hierarchical, position-based, and QoS-aware and network flow. Protocols that name data and ask questions based on certain characteristics fall into the data-driven category. In hierarchical category protocols, the nodes are divided into logical clusters. In each cluster, some nodes are considered as nodes and some as CH and the other nodes are considered as members of the cluster. Most of these protocols have two steps. The first stage is the selection of CH and the second stage is routing. The protocols that use positional information are categorized in positional category. Protocols that consider the quality of service and network flow, such as bandwidth and end-to-end and life-long delays are part of QoS category and network flow. Recent studies on the security of sensor networks indicate that the attention of most scholars is to providing low-cost, efficient, and secure solutions for the useful routing of WSNs. There are different definitions for the security of a sensor network, some of the most important of which are counterattack, eavesdropping, wormholes, black holes, and so on; thus, they try to increase the efficiency of the network. These quality parameters of the network are reducing the rate of lost packets, increasing the delivery rate of network packets, efficient energy, and so on overall leading to QoS in WSNs. In this study, the mechanism of trust management and methods of trust in the face of malicious attacks and incidents in WSNs were explained. After comparison and evaluation, we reached a comparative table of the most important trends and parameters effective in creating, maintaining and supporting the trust mechanism. Moreover, the trust-based routing protocol was explained. OLSR protocol was described and its characteristics were enumerated. The process steps were described. The packets in the protocol were described and the security challenges of the protocol were stated, and the defense approach against these challenges was tabulated. Thus, we paved the way for future studies in this regard to apply protocols to enhance the selection and performance of trusts as required.

References

[1] Nishimura, C., E. and D.M. Conlon. 1994. IUSS Dual Use: Monitoring Whales and Earthquakes Using SOSUS. Proceedings of the Mar. Tech., Soc. Journal, Vol. 27, No. 4, pp. 13-21.

[2] Ilyas, M. and I. Mahgoub. 2005. Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. Proceedings of the CRC Press, London, Washington, D.C.

[3] Akyildiz, I.F., W. Su, Y.Sankarasubramaniam and E. Cayircl. 2002. A survey on sensor networks. Proceedings of the IEEE Communication Magazine, Vol. 40, pp. 102-114.

[4] Goldsmith, A.J. and S.B. Wicker. 2002. Design challenges for energy-constrained ad hoc wireless networks. Proceedings of the IEEE Wireless Commun, pp.8–27.

[5] Al-Karaki, J.N. and A.E. Kamal. 2004. Routing techniques in WSNs: a survey. Proceedings of the IEEE Wireless Communications, Vol. 11, pp. 6-28.

[6] Akkaya, K. and M. Younis. 2005. A survey on routing protocols for WSNs. Proceedings of the Elsevier Ad Hoc Network Journal, pp. 325-349.

[7] Hedetniemi, S. and A. Liestman. 1988. A survey of gossiping and broadcasting in communication networks. Proceedings of the Networks, Vol. 18, no. 4, pp. 319–349.

[8] Heinzelman, W., A. Chandrakasanand H. Balakrishnan. 2000. Energy-efficient communication protocol for wireless mi-crosensor network. Proceedings of the IEEE System Sciences, pp.1-10.

[9] Heinzelman, W., J. Kulik and H. Balakrishnan. 1999. Adaptive protocols for information dissemination in WSNs. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_99), Seattle, WA.

[10] Shah, R. and J. Rabaey. 2002. Energy aware routing for low energy ad hoc sensor networks. Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, pp.350-355.

[11] Kulkarni, S., A. Iyer and C. Rosenberg. 2006. An Address-Light, Integrated MAC and Routing Protocol for WSNs. Proceedings of the IEEE/ACM Transactions on Networking, Vol. 14, no. 4, pp.793-806.

[12] Bulusu, N., J. Heidemann and D. Estrin. 2000. GPS-less low cost outdoor localization for very small devices. Proceedings of the IEEE Personal Communications Magazine, Vol. 7, issue. 5, pp. 28-34.

[13] Moore, D., J. Leonard, D. Rus and S. Teller. 2004. Robust distributed network localization with noisy range measurements. Proceedings of the ACM SenSys, pp. 50-61.

[14] Roosta, T. 2005. Probabilistic geographic routing protocol for ad hoc and sensor networks. Proceedings of the Wireless Networks and Emerging Technologies.

[15] Xu, Y., J.S. Heidemann and D. Estrin. 2001. Geography-informed energy conservation for ad hoc routing. Proceedings of the Mobile Computing and Networking, pp. 70-84.

[16] Salzmann, J., S. Kubisch, F. Reichenbach and D. Timmermann. 2007. Energy and Coverage Aware Routing Algorithm in Self Organized Sensor Networks. Proceedings of the Networked Sensing Systems. INSS '07. Fourth International Conference on Publication, 6-8.

[17] Liu, R.P., G. Rogers, S. Zhouand J. Zic. 2007. Topology control with Hexagonal Tessellation. Proceedings of the International Journal of Sensor Networks Vol. 2, No.1/2, pp. 91 – 98.

[18] Akl, R. and U. Sawant. 2007. Grid-based Coordinated Routing in WSNs. Proceedings of the Consumer Communications and Networking Conference, CCNC 2007. 4th IEEE Publication, pp. 860-864.

[19] Zhang, Z. 2006. An Enery Efficient Data Query Protocol for Wireless Sensor Network Applications. Proceedings of the PSC, pp. 61-70.

[20] Ye, F. 2001. A scalable solution to minimum cost forwarding in large sensor networks. Proceedings of the IEEE 10th International Conference on Computer Communications and Networks (ICCCN), Dallas, pp. 304-309.

[21] Sohrabi, K. 2000. Protocols for self-organization of a wireless sensor network. Proceedings of the IEEE Personal Communications, Vol. 17, no. 5, pp. 16–27.

[22] Zhan, G., Weisong Shi and Julia Deng. 2012. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2.

[23] Li, X., M.R. Lyu, L. Jiangchuan. 2004. A Trust Model Based Routing Protocol for Secure Ad hoc Networks. IEEE Proceedings on Aerospace Conference, vol. 2

[24] Babu, S.S., A. Raha, M.K. Naskar. 2011. Trustworthy Route formation Algorithm for WSNs. International Journal of Computer Applications (0975 – 8887) Volume 27– No.5.

[25] Zahariadis, T. and (et al). 2010. Trust management in WSNs. European Transactions on Telecommunications 21.4: 386-395.

[26] Weifang1, C., L. Xiangke1, S. Changxiang2, L. Shanshan1 and P. Shaoliang1. 2006. A Trust-Based Routing Framework in Energy-Constrained WSNs. X. Cheng, W. Li, and T. Znati (Eds.): WASA, LNCS 4138, pp. 478 – 489. © Springer-Verlag Berlin Heidelberg.

[27] Marti, S., T. Giuli, K. Lai and M. Baker. 2000. Mitigating Routing Misbehavior in Mobile Ad hoc Networks. Proceedings of the Sixth Annual International Conference on Mobile Computingand Networking (MobiCom). ACM Press, pp. 255–265.

[28] Pirzada, A.A., A. Dattaa and C. McDonald. 2006. Incorporating trust and reputation in the DSR protocol for dependable routing. Computer Communications Volume 29, Issue 15, Pages 2806-2821

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

[30] Michiardi, P. and R. Molva. 2002. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, vol. 228. Kluwer Academic Publishers, pp. 107–121.

[31] Pirzada, A.A. and C. McDonald. 2007. Trusted Greedy Perimeter Stateless Routing. IEEE, ICON.

[32] Tanachaiwiwat, S., P. Dave, R. Bhindwale and A. Helmy. 2004. Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks. IEEE International Conference on Performance, Computing, and Communications.

[33] Perrig, A., R. Szewczyk, J.D. Tygar, Victorwen and David E. Culler. 2002. SPINS: Security Protocols for Sensor Networks. ACM Journal of Wireless Networks, 8:5, pp.521-534.