Energy-aware Clustering with Variable Ranges in Wireless Sensor Networks

Faruk Bagci
Department of Computer Science and Engineering
German University in Cairo
Cairo, Egypt
Email: faruk.bagci@guc.edu.eg

***Abstract*—Traditional wireless devices communicate directly with a beacon or base station located in range of the device. Multi-hop messages are still a rarity in wireless communication. Wireless sensor network protocols often are based on peer-to-peer infrastructure, where messages traverse long distances through the network to reach a certain destination. A flat infrastructure is hard to manage regarding routing and scalability, if number of nodes increase drastically. Because of battery operated nodes, energy-effective mechanisms are very important in wireless sensor networks. Clustering brings hierarchy into the network and can save energy since nodes within a cluster usually communicate locally in a short range. Messages sent to large distances are handled by cluster-heads routing them through an inter-cluster backbone. A heterogeneous infrastructure with a large number of simple and cheap sensor nodes and only a small percentage of more powerful cluster-heads is beneficial but not necessary. This paper presents a new clustering approach called *Variable Ranges Protocol* that provides basic features to modify the range of each node. A dynamic transmission range adaption protocol substantially prolongs the lifetime of the nodes through energy efficient communication without significantly decreasing the node connectivity. The VR protocol is implemented combining several MAC protocols for local communication within a cluster.**

***Keywords*-Wireless sensor network; cluster architecture; energy efficiency; connectivity; wireless communication;**

I. INTRODUCTION

The study of sensor networks, while being a research field in and of itself, forms a basis for various areas where the collection of environmental data through sensors is essential (*e. g.*, security, traffic control, ubiquitous computing, *etc.*). The combination of sensing/sensoring, computational aspects, and communication solutions provides for a broad range of applications such as smart hospitals, intelligent battlefields, earthquake response systems, and learning environments [1] [2]. Generally, the term *sensor network* has come to describe a dynamically self-organizing collaborative network of widely distributed, tiny, low-cost, sensoring nodes ("smart dust") that are capable to cover an area and automatically communicate the collected data to a beacon or base station over multi-hop paths.

Sensor nodes are usually tiny, self contained, battery powered devices. Under normal circumstances it is impossible to replace or recharge these batteries, therefore the lifetime of a wireless sensor network is intrinsically restricted by the initially available power in each individual node, making power consumption considerations an essential part of any new protocol design. Similarly, very small memory, low processing power, and a limited communication bandwidth, all in comparison to traditional wireless devices, further restrict the options. Also, high failure rates, occasional shutdowns, and sporadic communication interference force continuous dynamic changes upon the topology. Finally, the sheer number of individual sensing devices of a sensor network, ranging from hundreds to thousands, make it infeasible to rely on previous solutions of ad-hoc networking protocols such as. For example flooding-based standard routing schemes for ad hoc networks simply do not scale adequately [3].

In [4] we proposed a security architecture for wireless sensor networks called *SecSens* which fulfills security requirements on multiple levels. SecSens focuses mainly on three security aspects: key management, secure routing, and verification of sensor data. The sensor network in SecSens consists of clusters, each containing a number of simple sensor nodes and one powerful node that acts as a cluster-head. Sensor nodes connect directly to the cluster-head, i.e. routing in clusters is not necessary. A node can be a member of several clusters at the same time. All cluster-heads form together an inter-cluster network used for sending messages to base stations. We assume that sensor nodes do not change their position once they are attached to a location. SecSens works with multiple base stations in order to avoid single-point-of-failures (see Figure 1). In the first version of SecSens clusters were built in the initial phase and remained unmodified for the whole lifetime of the network. Furthermore, all nodes used the same sending configuration, i.e. transmission power and range were set to maximum on each node. This paper describes an extension of this approach with dynamic features. The new variable ranges (VR) protocol optimizes the communication range of each node. This optimization results in more efficient usage of energy throughout the overall sensor network.

The next section describes related energy efficient communication approaches for sensor networks. Section III introduces the variable ranges protocol. We evaluated the new architecture in a wireless sensor network simulator. Section IV presents the evaluation results. The paper ends

 ISBN: 978-1-61208-144-1

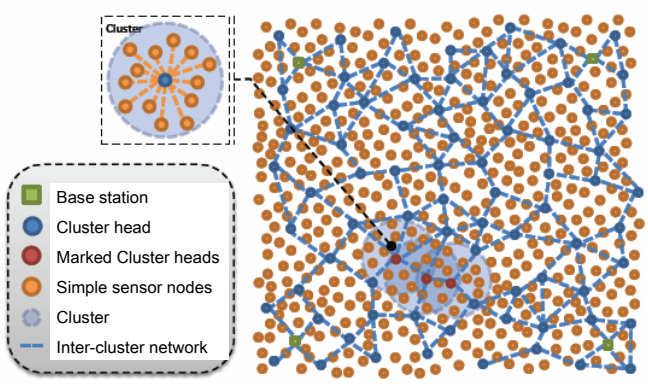


Figure 1. Basic sensor network architecture

with the conclusion.

II. Related Work

The Sensor-MAC (S-MAC) protocol [8] is an energy efficient communication protocol for wireless sensor networks. S-MAC is a slot-based protocol where each sensor node has alternating sleep and awake phases. The network is divided into clusters and all members of a cluster are awake or asleep at the same time. All cluster nodes exchange schedules in an initial phase. Within a cluster only one schedule is used, i.e. the schedule of the first node that sent a schedule. If a node receives multiple schedules it follows all of them. Such nodes have a higher energy consumption. Within an awake phase all cluster nodes contend with each other for medium access. The contention mechanism of S-MAC is the same as that in IEEE 802.11, i.e., using RTS (Request To Send) and CTS (Clear To Send) packets. S-MAC needs a strict timer synchronization in order to achieve correct functionality. Periodic synchronization among neighboring nodes is performed to correct their clock drift. An extension of S-MAC by *adaptive listening* is described in [9]. If a node A notices an ongoing communication of node B whom it wants to send a message, it sleeps the time until B is ready.

A modification of S-MAC called Timeout-MAC or T-MAC is introduced in [10]. In S-MAC all nodes need to be awake in the contention phase even if they have nothing to send or receive. T-MAC uses a specific timer T_A to shorten the awake phase if the node does not need to communicate. Obviously the T_A is smaller than the contention phase, thus the energy consumption is reduced. But if the timer T_A is chosen too small, the node sleeps early missing possible message requests of other nodes. This *early sleeping problem* could even lead to unfairness. In further extensions of T-MAC this problem is solved by *future request to send (FRTS)* messages, but this increases again the energy consumption. Nevertheless T-MAC gains better energy results compared to S-MAC.

Token ring [11] can be classified as a combination of TDMA and contention-based. Each node has its own time slot (token holding time) where it has to manage the communication with multiple contending nodes. The *Wireless Token Ring Protocol (WTRP)* [12] was developed for mobile ad-hoc networks. All nodes build a single ring in the initial phase. The aim of WTRP is to maximize the throughput and minimize the latency without restraining the mobility. Energy efficiency is not considered in WTRP because the nodes are mobile devices with strong energy resources like Laptops or PDAs. A mapping of WTRP on wireless sensor networks is *E^2WTRP* that is described in [13]. E^2WTRP aims to enhance the energy balance by dynamic adaptation of the token holding time. An active node can send more messages if the token holding time is increased. The frequency of token hand-over is decreased at the same time that reflects in lower energy consumption. *ESTR* [14] is an energy saving token ring protocol for wireless sensor networks that introduces sleep periods for nodes which does not need to send or receive messages. This leads to a very good energy balance.

III. Variable Ranges Protocol

A sensor node consumes most of the energy in its active mode. The energy cost rises enormously if the node uses radio communication. The energy consumption of the microprocessor Texas Instruments MSP430F149, which is used in several sensor boards, is 1.6 μA in sleep mode and rises to 280 μA in active mode at 1 MHz. In [8] the energy rate between active:receive:send is determined as 1:1.05:1.4, i.e. the energy consumption of sending a message outweighs other tasks. It is plausible that the energy consumption can be highly decreased by establishment of sleep intervals and avoidance of unnecessary packet sending. Using sleep intervals can lead to a contrary effect, i.e. the data exchange is reduced to a shorter time, which can cause higher packet collisions.

The energy consumption of sensor nodes that send with maximum transmission power lies significantly higher than with reduced power. Decreasing transmission power results in exponentially decreased energy consumption. Therefore, the Variable Ranges (VR) protocol saves energy by adjusting and optimizing the signal strength to particular circumstances of the sensor network in order to extend the lifetime of nodes. Additionally, the initial state of reduced transmission power of nodes ensures that complexity of network is low. With high signal strength nodes are confronted with frequent interferences and redundant paths within the network. Low signal strength means that number of neighboring nodes is less, i.e. probability for message collisions decreases.

Regarding the security architecture, the number of neighbors is also an important parameter. Each cluster-head has to manage several keys with each other neighboring sensor node and cluster-head for securing the communication

 ISBN: 978-1-61208-144-1

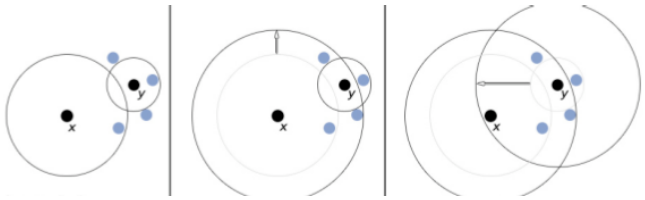


Figure 2. Range adjustment in VR protocol

and ensuring authentication. More neighbors means higher management effort and more storage space, as well as more encryption and decryption processing. All of this result again in increased energy consumption. Therefore, it is essential that the security architecture works hand in hand with the underlying communication protocol.

In the initial phase of the VR protocol, the nodes search for neighboring nodes starting with a minimum signal strength. For this reason, each node sends a *DiscoverNodes* message containing its own range parameter and ID. Then the node waits a certain time to get a response. The waiting time is also dynamic, i.e. the time is low, if the range is low and increases, if the range increases. The reason for this is that a node with a low range will reach less neighbors. Therefore, there is no need to wait a long time for a response. The nodes increase stepwise their transceiver power and send new discovery messages until a pre-configured number of nodes is found. A node which receives a *DiscoverNodes* message of an unknown node, extracts the range information of its seeking new neighbor. In the next step, the node compares the received range value with its own range. If the own range is lower, the node increases its range and sends a *DiscoverNodesReply* message back. Since the signal strength of the nodes would increase in this way until all nodes would settle at the range of the largest distance between two nodes, the VR protocol performs only a temporary range adjustment. This means that nodes discard the adaptation after a certain time and return again to their previous values.

Figure 2 illustrates this adjustment scheme. Assuming a maximum number of neighbors is set to three in this figure, it would be unfavorable for node y to use the range parameter of node x, since it can reach three neighbors with a much lower signal strength. For this reason, y will only increase range temporarily to answer node x and return to its previous range, in order to proceed with its own search. Cluster-heads find in this way a minimum number of other cluster-heads and as well as sensor nodes.

Actually, the aim of each cluster-head is to be reachable through the inter-cluster network by at least one base station. After the initial phase, each base station sends a broadcast through the new built network. This sink message is also important to generate new keys for further authentication. In [4] this key generation is described in detail. Therefore, reachability of base stations is essential to establish the security architecture in the sensor network. If a cluster-head does not receive a broadcast message after a certain time, it starts a new search phase to find new cluster-heads. The cluster-head uses this time a different message *DiscoverNewNodes*. It first uses the current range, since there could be cluster-heads which are in range, but not discovered. Cluster-heads who receive such a message, adjust their signal strength to answer, but keep their new range value this time. If the node does not get any answers, it increases its range and repeats the procedure until it finds new connections. Figure 3 shows the *TryToConnect* phase. You can see on the right side of the figure, that after the initial search phase, several local cluster networks are established, but not all of them can reach a base station marked here as green squares at the four corners. On the left picture you can recognize that the connectivity is enhanced after the *TryToConnect* phase, but nevertheless there are still local clusters remaining unreachable by any base station. The reason is that nodes are deployed randomly. There is a small probability that some nodes cannot reach a base station, even if transmission power is set to the maximum or due to message collisions in the initial phase.

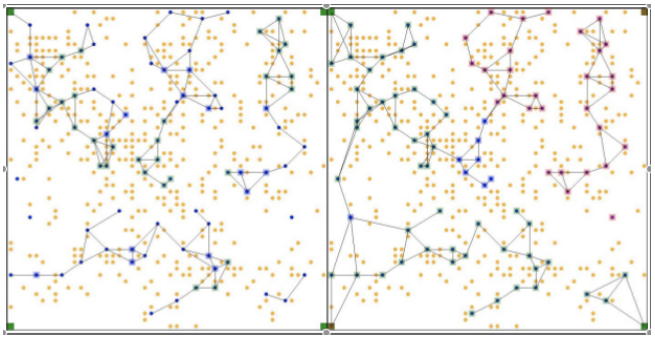


Figure 3. Initial phases of VR protocol: a) neighbor search b) TryToConnect

Cluster-heads check periodically their neighborhood for node losses or new arriving nodes. During lifetime the VR protocol ensures that nodes can dynamically adapt to changes in their environment. This network adaptation goes hand in hand with security adjustments.

Additionally, routing information is updated by cluster-heads after each VR adjustment phase. Simple sensors do not need routing capability, because they exclusively communicate with the cluster-head. Routing is used only within the inter-cluster network established by cluster-heads. Our architecture uses probabilistic multi-path routing based on the level values to forward messages from cluster-heads on the way to the corresponding base station. Cluster-heads build up a trust matrix, where each transmission to its neighbors is recorded. Based on this trust information, cluster-heads calculate a probability value and write it into the packet header. This value is used to decide in which direction the packet has to be send. Each cluster-head

 ISBN: 978-1-61208-144-1

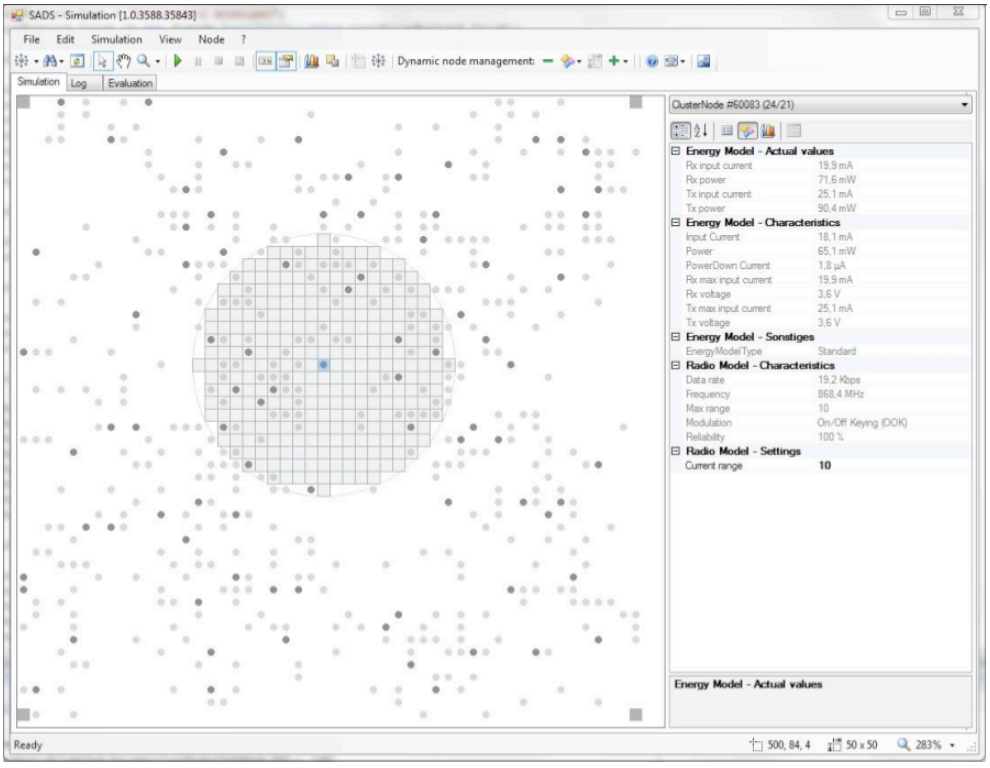


Figure 4. The Simulator GUI

modifies the probability value and sends the message over the most trustworthy route. Furthermore, our architecture provides passive participation, i.e. sensor nodes listen to packet transmissions of their neighbors. If cluster-head u detects a packet addressed to its neighbor v, and recognizes that v is not forwarding the message, u takes responsibility with a certain (low) probability. Also, if u assumes that v forwards the message to a non-existent node, u takes care of transferring.

IV. Evaluation

To evaluate the efficiency of our variable ranges security architecture we implemented a simulation tool where it is possible to establish different sizes of sensor networks. Figure 4 shows the GUI of the simulator. The simulation is divided into three phases: node distribution, initialization of network, and report sending. In the first phase, a predefined number of nodes is distributed randomly over a given area. Sensor nodes and as well as cluster-heads are deployed after setting for each a maximum transceiver range.

Basic parameters for the network are total number of nodes, initial node range, initial node energy, and network density. Type, range, and position of nodes can be changed easily using the simulator GUI. Furthermore, new nodes can be added or existing nodes can be deleted before the next phase of the simulation is started. Figure 4 shows a screenshot after the first phase. Dark circles are cluster-heads whereas light dots are simple sensor nodes. The squares at the corners represent again four base stations. In this case one cluster-head is selected and you can see the communication range of the current node.

The second phase initializes the network based on a communication protocol. We implemented three protocols that can be selected by the user in the beginning of this phase. These are the SMAC protocol, the energy saving token ring protocol (ESTR), and the variable ranges (VR) protocol. The user can change a set of parameters depending on the selected communication protocol, e.g. cluster size, timer settings, update periods. In this phase security and routing information is exchanged, too.

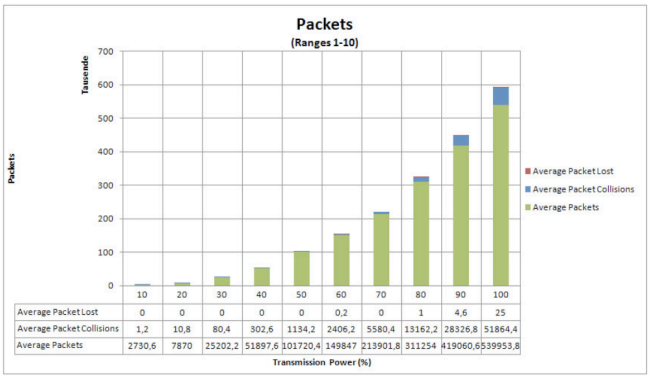
At the end of initialization, the network is established and nodes can start to exchange secured messages. This is simulated in the last phase by randomly generated reports that are sent to base stations. The user can halt the simulation at any time, in order to change parameters for nodes. For example, one can turn off a node to simulate a node loss. It is also possible to simulate a compromised node that sends false reports into the network.

Nodes consume energy for processing data, like encryption and decryption, and sending or receiving messages. For some communication protocols nodes can switch to a sleep mode, where energy consumption is minimal. Our simulator

 ISBN: 978-1-61208-144-1

bases on an energy model that uses specifications of real sensor boards: ESB 430/1 and MSB-430 of Freie University Berlin [15].

In a first evaluation we measured the number of messages sent in the initialization phase using the VR protocol. We performed several simulations where we modified the maximum range of nodes in order to get average number of sent packets, collisions, and lost packets. Figure 5 shows the results of a network with 500 nodes. Traffic load increase with higher range of single nodes, because nodes can reach more neighbors to exchange messages with.

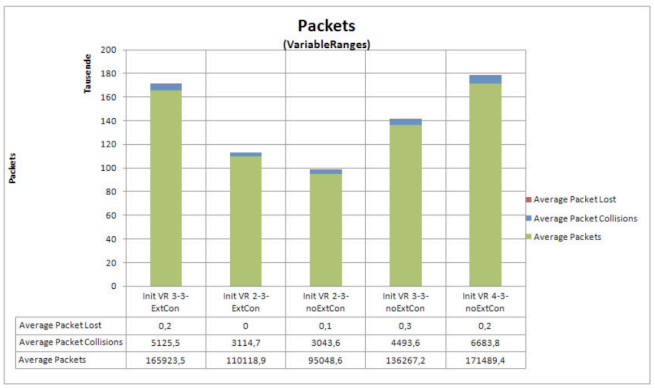


	10	20	30	40	50	60	70	80	90	100
Average Packet Lost	0	0	0	0	0	0,2	0	1	4,6	25
Average Packet Collisions	1,2	10,8	80,4	302,6	1134,2	2406,2	5580,4	13162,2	28326,8	51864,4
Average Packets	2730,6	7870	25202,2	51897,6	101720,4	149847	213901,8	311254	419060,6	539953,8

Figure 5. Traffic load in relation to signal strength

The VR protocol can be initialized with several parameters. As mentioned in the previous section, the VR protocol continues to search for new neighbors by increasing the transmission range. Using the simulator the user can set the maximum number of neigboring cluster-head and sensor for each node in the network, e.g. setting the number to three would stop the search after finding three cluster-heads in the neighborhood. In some cases, this would lead to a low connectivity, since nodes which could not join a cluster group would be disclosed. Therefore, VR protocol offers a second optimization step that was described in the previous section (*TryToConnect*). Figure 6 shows number of sent packets, packet collisions, and lost packets using different configurations of VR protocol. The notation *Init VR 3-3-ExtCon* means that each cluster-head searches for new neighbors until 3 other cluster-heads and 3 sensor nodes are found and the *TryToConnect* mode is turned on. It is clearly seen that packet collision in VR protocol is very low and there are nearly no packet losses, since the communication range is very reduced. The less packets are sent, the less energy is consumed. In Figure 6 the configuration *Init VR 2-3 noExtCon* seems to be the optimal configuration.

But regarding the connectivity this is not the best choice. Figure 7 shows the connectivity for each configuration. It is clearly seen that the connectivity for the configuration *Init VR 2-3 noExtCon* is only %14.15, i.e. only a small number of cluster-heads can actually reach a base station.



	Init VR 3-3-ExtCon	Init VR 2-3-ExtCon	Init VR 2-3-noExtCon	Init VR 3-3-noExtCon	Init VR 4-3-noExtCon
Average Packet Lost	0,2	0	0,1	0,3	0,2
Average Packet Collisions	5125,5	3114,7	3043,6	4493,6	6683,8
Average Packets	165923,5	110118,9	95048,6	136267,2	171489,4

Figure 6. Traffic load for different configurations of VR protocol

Turning on the *TryToConnect* modus brings only an increase of %10 in connectivity. Only after increasing the number of neighboring cluster-heads leads to reasonable results. Even without the second optimization phase, VR protocol can reach nearly %90 connectivity.

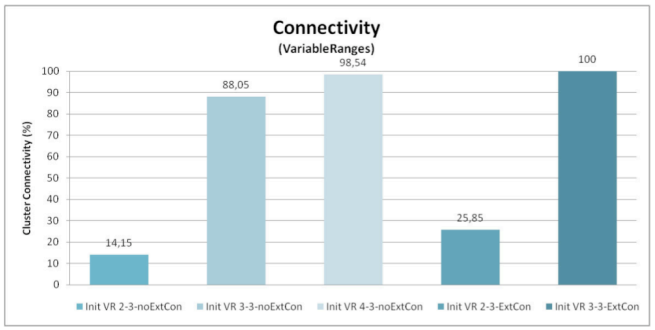


Figure 7. Connectivity for different configurations of VR protocol

As mentioned in the previous section, the complexity of sensor network is much lower using VR protocol. On the left side of Figure 8 the network was established with maximum node range. It is clearly seen that in dense areas of the network, the number of different connections is rather high. In a second simulation, we used the VR protocol to establish the network. As seen on the right part of Figure 8 using the VR protocol lowers the complexity of the network.

The optimal usage of signal strength in VR protocol shows its advantages also in energy consumption. Figure 9 illustrates the energy consumption for sending reports from a sensor node to the base station. Level represents here the distance between sending node and nearest base station, e.g. level 6 means that messages traverse six intermediate cluster-heads until they reach the base station. We performed the energy measurement in four different networks with the same size. For the first three networks the maximum range parameter of each node was set to a fixed value, i.e. range 6 stands for %60 maximum signal strength. The last

 ISBN: 978-1-61208-144-1

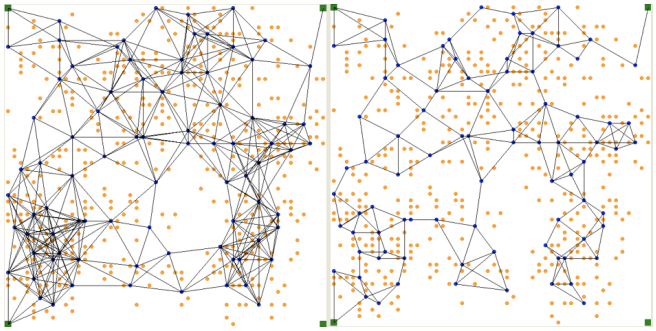


Figure 8. Network complexity without (left) and with VR protocol (right)

network used the VR protocol with at least three cluster-head and three sensor node neighbors and a further optimization step to increase the connectivity (*VR 3-3 ExtCon*). One can clearly see that the VR protocol has the best energy balance leading to a longer lifetime of the network.

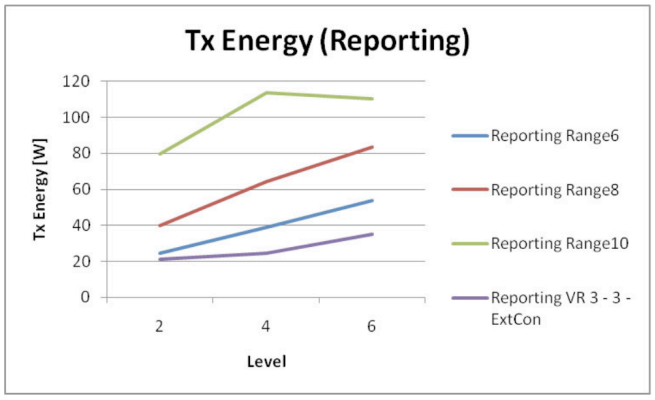


Figure 9. Energy consumption for reporting

V. Conclusion

This paper presented the Variable Ranges protocol for wireless sensor networks. Cluster architectures offer a good basis for scalable and energy-efficient protocols. Using hierarchy of cluster-heads and sensor nodes, it is possible to limit the range of each node and to exploit multi-hop communication. By dynamically adapting the range of each node, the network can be established with low complexity, but still with high connectivity. Since nodes do not sent messages with full transmission power, the energy consumption decreases considerably. This results in an extended lifetime of the overall sensor network.

References

[1] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," in *ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'02)*, Atlanta, GA, USA, September 2002.

[2] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, no. 5, pp. 51–58, 2000.

[3] P. Downey and R. Cardell-Oliver, "Evaluating the Impact of Limited Resource on the Performance of Flooding in Wireless Sensor Networks," in *Proceedings of the 2004 international Conference on Dependable Systems and Networks*, Washington, DC, USA, June 2004.

[4] F. Bagci, T. Ungerer, and N. Bagherzadeh, "Multi-level Security in Wireless Sensor Networks," *International Journal On Advances in Software*, vol. 4, no. 6, 2010.

[5] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[6] Donggang Liu and Peng Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks," *Trans. on Embedded Computing Sys.*, vol. 3, no. 4, pp. 800–836, 2004.

[7] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, New York, NY, USA, 2003, pp. 62–72, ACM Press.

[8] Wei Ye, John Heidemann, and Deborah Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," in *Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, New York, USA, June 2002, vol. 3, pp. 1567–1576.

[9] W. Ye, J. Heidemann, and D. Estrin, "Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, pp. 493–506, June 2004.

[10] Tijs van Dam and Koen Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*, Los Angeles, California, USA, Nov. 2003, pp. 1567–1576.

[11] IEEE, *IEEE CS, Token Ring Access Method and Physical Layer Specifications. ANSI/IEEE Standard 802.5*, 1985.

[12] M. Ergen, D. Lee, R. Sengupta, and P. Varaiya, "WTRP - Wireless Token Ring Protocol," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 6, pp. 1863–1881, Nov. 2004.

[13] Zhenhua Deng, Yan Lu, Chunjiang Wang, and Wenbo Wang, "E^{2}WTRP: An Energy-Efficient Wireless Token Ring Protocol," in *Proceeding of the IEEE conference on Personal, Indoor, and Mobile Radio Communications*, Barcelona, Spanien, 2004, pp. 398–401.

[14] F. Bagci, T. Ungerer, and N. Bagherzadeh, "ESTR - Energy Saving Token Ring Protocol for Wireless Sensor Networks," in *Proceedings of the International Conference on Wireless Networks (ICWN '08)*, Las Vegas, NV, USA, July 2008.

[15] http://www.scatterweb.com, *ScatterWeb Homepage*, 2007.

 ISBN: 978-1-61208-144-1