Simulation and Evaluation of CTP and Secure-CTP Protocols

Peter PECHO, Petr HANÁČEK, Jan NAGY

Faculty of Information Technology, Brno University of Technology, Božetěchova 2, 612 66 Brno, Czech Republic

pecho@fit.vutbr.cz, hanacek@fit.vutbr.cz, inagy@fit.vutbr.cz

Abstract. *The paper discusses characteristics and qualities of two routing protocols – Collection Tree Protocol and its secure modification. The original protocol, as well as other protocols for wireless sensors, solves only problems of radio communication and limited resources. Our design of the secure protocol tries to solve also the essential security objectives. For the evaluation of properties of our protocol in large networks, a TOSSIM simulator was used. Our effort was to show the influence of the modification of the routing protocol to its behavior and quality of routing trees. We have proved that adding security into protocol design does not necessarily mean higher demands for data transfer, power consumption or worse protocol efficiency. In the paper, we manifest that security in the protocol may be achieved with low cost and may offer similar performance as the original protocol.*

Keywords

Routing protocol, wireless sensor networks, security.

1. Introduction

The paper proposes modifications of the routing Collection Tree Protocol (CTP) [2] with regard to the essential security objectives. We were interested in how the protocol modification influences the quality of the routing path and the amount of radio communication. Our goal was to prove that such modification does not necessarily lead to worse performance.

1.1 Wireless Sensor Networks

Wireless sensor networks (WSNs) are typical examples of computation and energy constrained devices. Sensor nodes are mostly powered by alkaline AA batteries, that are not rechargeable and therefore their working time is usually short, typically several weeks (or several months in case of using expensive D lithium batteries) [3]. Radio communication of nodes is usually unreliable and belongs to the most energy consuming tasks. Common network protocols are not suitable for this kind of networks, thus special protocols are needed. Such protocols have to transmit minimum amount of data and (in most applications) information about infrastructure is not available in advance .

One of today's standard platforms for low-cost sensor networks is TinyOS [5], which is currently distributed in version 2.x. The last stable version 1.x is, however, still often used. The organization developing this low level operating system for sensor networks, TinyOS working groups, is publishing technical papers about protocols and schemes for sensor networks – TEP (TinyOS Enhancement Proposals) [5]. One of the TEPs describes Collection Tree Protocol (CTP), which is a routing protocol suitable for sensing applications. The CTP is also distributed as a part of TinyOS-2.x [2].

1.2 Collection Tree Protocol

The Collection Tree Protocol (CTP) is a simple tree-based protocol proposed for collection of data from sensor nodes into the root node. All the communication is many-to-one or one-to-many. The nodes form a set of routing trees, whereas multiple root nodes are allowed. The CTP is address-free protocol. The sensors send data packets to the next hop whereas routes are based on a routing gradient. The protocol has the following properties [2]:

- CTP assumes that it has link quality estimates of some nearby neighbors. These provide an estimate of the number and quality of transmissions it takes for the node to send a unicast packet whose acknowledgment is successfully received.
- CTP has several mechanisms to improve delivery reliability, but it does not promise 100 % reliable delivery. It is best effort, but a best effort that tries very hard.
- CTP is designed for relatively low traffic rates. Bandwidth-consuming systems might benefit from a different protocol, which can, for example, pack multiple small frames into a single data-link packet.
- CTP uses expected transmissions (ETX) as its routing gradient. A root has an ETX of 0. The ETX of a node is the ETX of its parent plus the ETX of its link to its parent. If several routes are valid, CTP should choose the one with the lowest ETX value.

This protocol was proposed for data gathering with low energy demands. Routes established during node deployment are not updated periodically, but only if inconsistency in the network topology is detected. A loop is detected when node chooses a route with gradient value significantly higher then its old one. This may be caused by losing connectivity with the current parent node. The CTP offers two solutions: (1) beacon frame and (2) ignoring routes with an ETX higher than a reasonable constant. The protocol provides also a handle for packet duplication. When a duplicate instance of a packet is detected during its forwarding, it is dropped.

The CTP is designed in the light of minimum power consumption and the only considered threats were unintentional threats. Is has no countermeasure against a motivated attacker and therefore its implementation into applications used in hostile environment is usually unacceptable. Our aim was to propose such improvement of CTP that offers high network protection at the cost of small energy overhead.

1.3 Sensors with Tamper-Resistant Modules

Wireless sensors used in practical applications are usually low-cost, low-power and small-size devices mostly without any essential physical protection. Each improvement of covering, computing performance or sensors leads to the higher price or higher demand of power resources [4]. Wireless sensor networks used in a hostile environment are highly vulnerable to any physical manipulation. As the sensor nodes provide many input/output channels together with hidden channels, it is almost impossible to design reliable data protection. Tamper-resistant covering is able to protect computational core of the sensor node, however attached sensors for sensing parameters of hostile environment are still unprotected. Thus, it is better to define tamper-resistant sensor node as a sensor node composed of two portions: (1) common sensor node hardware as the tamper-vulnerable portion and (2) tamper-resistant module.

Our previous work ([6, 7]) was concerned to design secure but low-cost sensor node platform. The concept of the platform is based on wiring of sensor node with a tamper-resistant module. Our results have been proved in real hardware and have shown that by using specialized hardware, we can reduce power consumption and improve the security at small cost. This is important especially for effective implementation of asymmetric and strong symmetric cryptography, that belongs to the most complex algorithms for sensor nodes. When the concept of partially tamper-resistant sensor nodes was proved, we proposed a modification of the CTP to utilize the security properties of the platform.

2. Secure Collection Tree Protocol

The Secure Collection Tree Protocol (Secure-CTP) was designed for sensor nodes with tamper-resistant modules [7]. Smart cards offer best benefit-price ratio, thus are used a tamper-resistant modules. Connection of the smart card and node micro-controller is realized by serial interface. Radio communication channel is considered to be non-trustworthy. The smart card is powered up only for cryptographic operations. If the sensor is in idle mode, the smart card is turned off.

The most significant changes in the Secure-CTP protocol are (1) usage of a unique 16-bit identifier, (2) modified usage of ETX, (3) usage of Routing Frame Counter and (4) usage of Message Authentication Code (MAC) used for providing integrity and authentication. Each sensor node has a unique, 16-bit identifier stored in the smart card (ID). The identifier is read-only and is defined during production time of tamper-resistant sensors. Each transmitted frame has the ID of last hop sensor and message authentication code attached. The smart card also holds master key (shared by all smart cards in the network) and monotonic counter. The master key never leaves smart card and may be used only as a parameter of cryptographic routines. This key together with node identifiers is used for generation of the session key and thus it never leaves the smart card as well.

When the node receives a routing frame with better routing path, the frame is forwarded to smart card together with link quality estimation to the source node. In the smart card, a session key is generated from the master key, source ID and current node ID. This key is used for validation of MAC of the original routing frame and after modification of ETX also for generation of the new MAC. This new frame is then forwarded back to the sensor board.

Data security is provided by symmetric cryptography, as probably all ISO/IEC 7816 smart cards offer 3DES or AES encryption at high speeds. The chosen encryption algorithm defines 64-bit data blocks. Key length is 112 bits for 3DES and 128 bits for AES. Integrity of the frames is protected by CBC-MAC [8]. From the 64-bit MAC, only the last 32 bits are used. Frames without MAC are dropped.

Routing frames are protected by 32-bit monotonic routing frame counter (RFC). Sensor node accepts routing frame with a higher value of counter, or with a lower value, but the difference is within an allowed range. Routing packets with other counter value are dropped. Recommended allowed range of RFC is from 2^8 up to 2^{10}. This range enables synchronization, if the sensor node had received broken packets because of radio transmission problems. Lower values could cause synchronization problems, higher values could be misused to counter overflow. New sensor node added to the network has not received any RFC before. Thus, a special flag inside secure memory is set to indicate that any RFC from a valid routing frame may be accepted.

ETX value of the last routing frame is stored in secure storage and it is incremented in a limited range. This modification in contrast to CTP enables only to increment ETX by 1, 2, or 3 bits (that means 1-2, 1-4, or 1-8), depending

on implementation. We suppose that using more bits for link estimation does not have significant influence. Root nodes may initiate re-establishment of routing tables. They are the only nodes that could create zero ETX routing frames. When inconsistency of routes is detected, the nodes should inform the root node by sending a beacon frame. This frame has to be protected by MAC to avoid beacon frame injection. Root node responds to received inconsistency by sending routing frames with zero ETX.

2.1 Frame Formats

Communication architectures for networked sensors are mostly based on the Active Messages model [9]. This layer is used as a network layer for CTP and Secure-CTP protocol. Active message frame (Fig. 1) is used for transportation of any higher level frame.

In the Secure-CTP we proposed the following changes: addition of (1) RFC and (2) MAC to the Routing Frame. In contrast to the CTP, we also defined addition of last hop ID and frame counter. In the implementation of CTP in TinyOS-2.x, frame counter is already used, however it's not mentioned in the specification. Modifications of the routing frame format can be seen in Figs. 3(a), 3(b) and 3(c). Beacon frame format is missing in the CTP specification as well. Thus, for the simulation of the CTP and Secure-CTP we have used the same format – see Fig. 2.

2.2 Security

Our goal was to propose such modifications that fulfill at least the essential security requirements. In case of routing protocol, the most important are authentication, integrity and freshness. If the routing protocol provides these services, the attacker cannot affect establishment of routing paths.

Confidentiality is usually not necessary for routing protocols, as the routing path is not a sensitive information. Moreover, wireless sensor networks based on 802.15.4 cannot guarantee availability as the radio channel may be jammed. Cryptographic mechanisms of Secure-CTP satisfies these essential security goals.

3. Link Quality Estimation

We must also mention that despite of high frame error rate (FER) between very far nodes, while transmitting thousands of frames, it's highly probable that some nodes capture also frames from low-quality channels. Therefore, each routing protocol has to employ some distance function for evaluation of radio channel quality. Current sensor nodes do not offer link quality estimator implemented in hardware. There are also no direct information from the hardware about invalid received frames. Thus, software link estimators have to use frame counters, which also prolongs the frames.

Routing protocols for ad-hoc networks need to evaluate the quality of paths to the other nodes. Frames are transmitted over the nodes with $(1-FER)$ probability, whereas signal strength descents by the square of the distance. Quality of the channel in the routing protocol is given by the chosen link estimator or by the chosen algorithm. The CTP does not define link quality calculation, however its implementation in TinyOS-2.x uses LinkEstimator library, that is supplied with the TinyOS-2.x. Link quality is directly used for calculation of the ETX. In the specification, there is also no information about prolonging of transmitted frames by the LinkEstimator library.

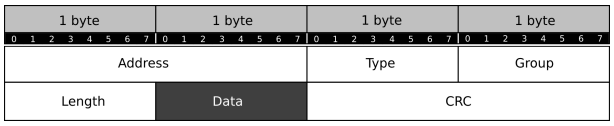


Fig. 1. Active message frame format.

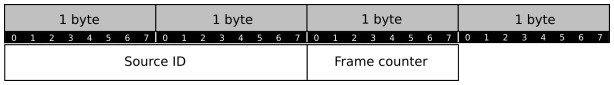
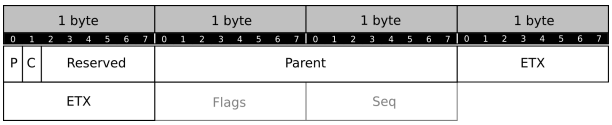
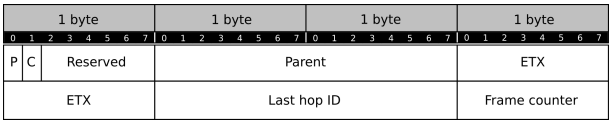


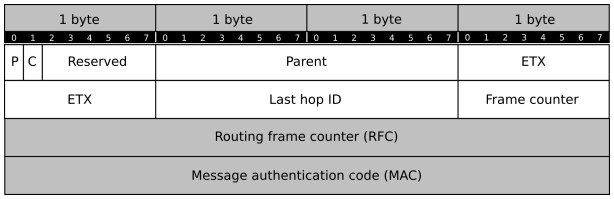
Fig. 2. Beacon frame format.



(a) Routing frame format of CTP according the specification.



(b) Routing frame format of CTP from the simulation.



(c) Routing frame format of Secure-CTP.

Fig. 3. Routing frame format of CTP and Secure-CTP.

Due to unavailability of this library for TinyOS-1.x, we have defined our own link estimator that was used in both protocols, CTP and Secure-CTP, to do proper evaluation and comparison of protocol characteristics. Original implementation of LinkEstimator library from TinyOS-2.x appends a special header to each transmitted frame. Upper 8 bits of the header are used as flags, lower 8 bits are used as a frame counter. Our implementation of the link estimator appends a 16-bit last hop ID and 8-bit frame counter, which is 8 bits more than the original protocol. However, we do not assume any significant changes in behavior in comparison to implementation in TinyOS-2.x.

The frame counter is unique for each node and is used for calculation of (1) all transmitted frames, (2) number of received frames from each node and thus (3) the link quality. Each node holds these counters and parameters for all

neighbor nodes. During the implementation, we have found that 8 bits per counter offers sufficient precision for quality calculations. If the counter of received frame would overflow by receiving the next frame, all counters for given node are divided by 2 (or shifted by 1 bit to the right). This operation also serves for elimination of older link quality information.

Link quality is then given as:

$$ETX = \frac{frames_{recv} * 256}{frames_{total}}. \quad (1)$$

ETX for Secure-CTP is reduced to 1 – 3 bits in consideration of probabilistic distribution of the link quality in the simulated network.

4. Protocol Evaluation Methodology

Radio communication interface, also used in WSNs, suffers from unreliability and communication collisions. Each protocol designed for radio ad-hoc networks has to be designed with regard to these restrictions. Moreover, sensor nodes have very limited power sources, so the communication should be as effective as possible. Each transmitted or received byte shortens the network lifetime. Current sensor nodes mostly use radio controllers that consume the same energy for transmitting and capturing the frames [10]. Thus, any unnecessary transmission withdraws energy of sending node as well as receiving the frames. This is important especially for broadcast communication, when not only the frame header, but rather the whole frames are received – see active message format.

During design of a new routing protocol, it is rather difficult to find the most effective path with regard to power consumption. Long hops are less reliable and the frames need to be retransmitted, but the retransmission of lower amount of frames spends less energy. On the other hand, multiple short hops may offer higher reliability, so minimum of frames needs to be retransmitted. Higher number of hops and frames, however, may also cause higher power consumption.

Routing protocols may also be evaluated in the light of volume of transmitted data, length of the routing paths, necessary time for establishment of routing paths, reliability of routing trees, security objectives and others. For this evaluation, we have compared the routing protocols with regard to power consumption. The routing tree established by CTP is considered as the best solution. The protocols are compared with regard to the volume of transmitted and received bytes, that may be directly used for calculations of consumed energy. We were also focused on the number of frames necessary for establishment of the whole routing tree.

Sensor networks platform does not offer additional information about collisions during frame transmission, thus we do not know how much energy was spent for an unsuccessful transmissions. For this evaluation we will consider that each collision has occurred in the middle of the transmission.

5. Simulation Model

Evaluation of the protocol may be done by formal analysis or using a simulation. For our purpose we have chosen the second method, as we were interested in behavior of the protocol in large scale networks. For simulations we chose TOSSIM, a discrete event simulator for TinyOS sensor networks [1]. The simulator implements a radio stack that is almost identical to the MICA* 40Kbit RFM-based stack. Thus it may be used for evaluation of radio communication including collisions. Limited radio range is modeled by a lossy radio model, whereas a directed graph defines the probability of receiving a corrupted bit. This characteristic of communication among the nodes is also known as the bit error rate (BER).

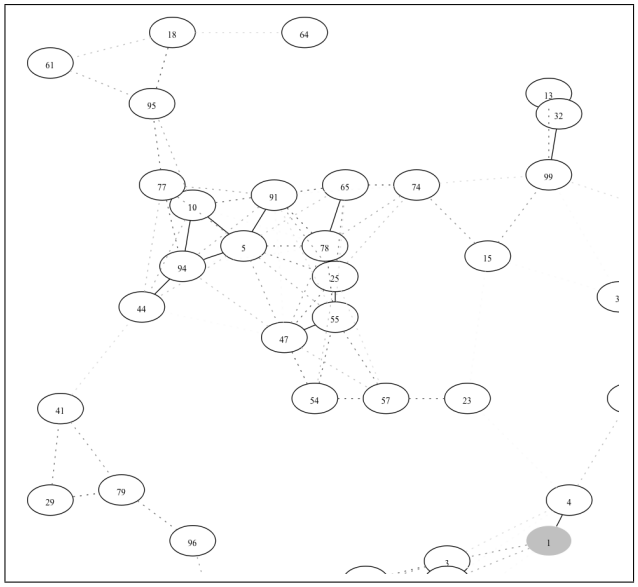


Fig. 4. Distribution of Nodes for Sensor Network Simulation.

The TOSSIM is distributed with a generator of lossy radio model, which creates models according to the BER value. However, it does not offer information about node positions that are necessary for evaluation of routing protocol. We designed and implemented another configurable generator of radio lossy model. This generator gives the radio model as well as a graphical representation of sensor node distribution. Using such information, it is possible to evaluate routing protocol for correctness and efficiency of the implementation. In Fig. 4, you can see the simulated sensor network with highlighted best communication channels.

Our aim was to evaluate the establishment of the routing tree and the effectiveness of this process. We were interested in different behavior of CTP and Secure CTP, especially in the influence of the protocol modification to:

- Quality of routing paths and volume of radio communication,
- collisions in the radio communication (due to extended routing frames),
- quality of routing paths depending on ETX length,
- convergence of quality of routing paths.

We did not implement nor simulate any application protocol. In case of simulation or communication in a real application, the results depend on node deployment, application type and characteristics of the environment. Therefore, we were only focused on the process of establishment of the routing tree.

Extending the transmitting frames usually leads to overhead of radio communication. Moreover, any changes in the routing scheme may also lead to unpredictable behaviour. We were focused on propagation of actual value of RFC in the sensor network as this step has a direct influence on rescission of the forwarded routing information. Because of unreliable radio communication, nodes in the same location may hold various values of RFC at the same time. Different locations of the sensor network may hold much different RFC, so it's not likely that nodes successfully forward the routing information to distant locations.

For simulation purpose we use a sensor network that consists of 100 nodes with minimum distance median of nodes of 5.0 length units and maximum communication distance of 200 length units. The same deployment of nodes was used for evaluation of CTP and Secure CTP protocol. Each simulation consists of 10 runs and the results were statistically processed. Each simulation takes 60 virtual seconds and the sensor nodes boot over the first 10 seconds. The achieved results were validated by two runs of simulations.

Simulation model implements one retransmission of broken frames to improve radio reliability. If we consider a link of 99 % BER and 16-byte frame, this improvement decreases the FER from 72.3 7% to 52.37 %. An example of an established routing tree can be seen in Fig. 5.

6. Evaluations

At first we were interested in distribution of reliability of link qualities and thus calculation of effective ETX. We tried to find out if the whole range of ETX is already used. Afterwards, we focused on protocol communication during routing tree establishment, especially the amount and type of received and sent frames. During the simulation we observed a dependency of transmitted data to the number of established route paths. We supposed linear dependency. We were interested in influence of the modified, and particularly longer, frames on the number of radio collisions during the transmission. All three variants of Secure-CTP with 1, 2, or 3-bit ETX were tested.

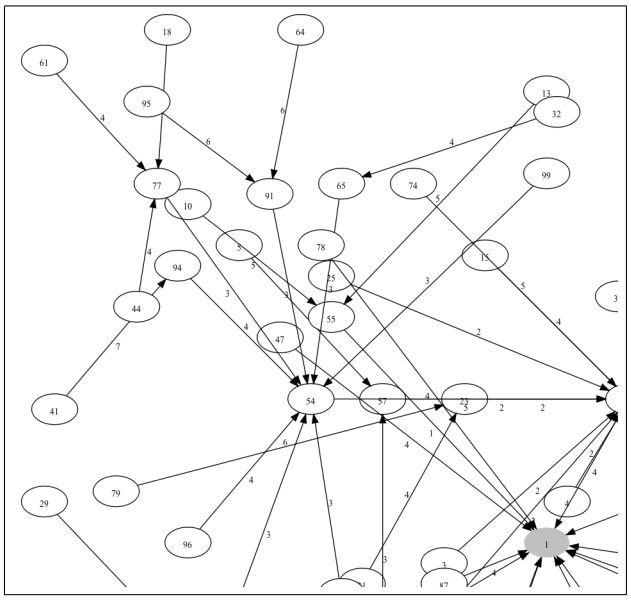


Fig. 5. Example of Established Routing Tree Using S-CTP with 2-bit ETX.

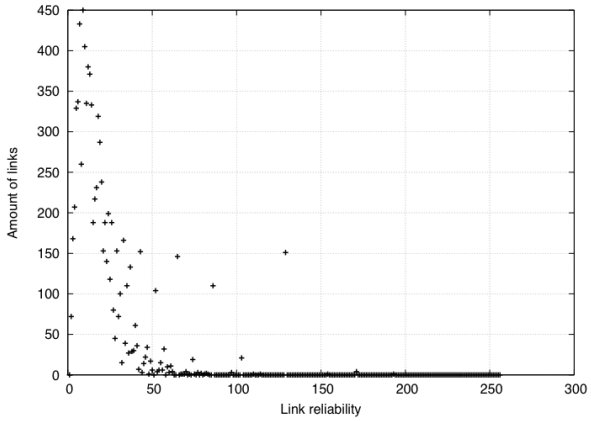


Fig. 6. Dependency of number of links on their reliability.

6.1 Calculation of ETX

Calculation of ETX is important for Secure-CTP protocol, as this protocol tries to use the minimum range of ETX. Using the simulation we tried to find statistics of reliability of the links between sensor nodes. In Fig. 6, you can see the statistics of link qualities gained from the simulations. In the graph a poisson distribution of link qualities can be seen. 95 % of all links reach the value of 64 on average. To minimize the ETX range, only a few bits can be used. Next in the simulation, we tried to find out the influence of ETX length on the routing tree and the process of its establishment as well. In the implementation, only the lower 6 bits are used (i.e. 0 – 63). Better quality links saturate in this range.

6.2 Amount of Radio Communication

In the next part, we focused on the amount and type of frames necessary for establishment of routing paths to the

10 %, 50 %, 90 % and 100 % of network nodes. The number of transmitted and received bytes directly determines the consumed energy.

Results of this simulation has shown that adding security to the CTP protocol has a small influence on the total received and transmitted bytes. In Tab. 2 you can see the number of received and transmitted beacon frames (BF) and routing frames (RF), as well as the total amount of bytes processed by the radio subsystem. The statistics are counted for 10 %, 50 %, 90 % and 100 % of established paths. Each simulation was taken twice and consists of 10 simulation runs. The simulations were evaluated independently, whereas number of simulation run is also in Tab. 2. To reduce random factors, median and standard deviation of each simulation were computed.

Random factors may cause collisions in radio communications. In the beginning of routing tree establishment, the nodes can start communication at the same time. That may lead to communication overhead as the frames need to be re-transmitted. That is why the number of frames may significantly differ between the simulation runs.

In case of CTP there are a lot of small frames transmitted, while in case of Secure-CTP a smaller number of larger frames is transmitted. We believe that this behavior is caused by adding the RFC to the routing frame, thus older routing frames are dropped more often. We have found that modified usage of ETX has minimal effect on the process of routing tree establishment. The length of ETX has also no significant impact on the amount of data.

In the graph (Fig. 7), there is a dependence of the established paths on the total received and transmitted data. It is evident that the amount of communication rises exponentially. The most of transferred data can be seen for the last 10 % of nodes. Energy needed to establishment of these paths is similar to amount of energy necessary for establishing paths to the previous 90 % percent. This energy is slightly higher for Secure-CTP however the difference is irrelevant. We suppose this is probably caused by distribution of different value of RFC through the network. The shift of the Secure-CTP with 1-bit ETX in graph may be caused due to random effects, however the trend is similar to other variants of Secure-CTP.

6.3 Collisions of Radio Communication

One of the most significant changes in Secure-CTP is extending the frames, which may have influence on the higher amount of collisions of radio communication. Results of the simulation (Tab. 1) has shown, that Secure-CTP does not suffer from more collisions than the CTP. Thus, in the next calculations we did not take into account collisions during data transmission. We believe that lower amount of collisions is the consequence of lower amount of transmitted frames due to usage of RFC. In all the calculations the simulation time was included, which is 60 virtual seconds.

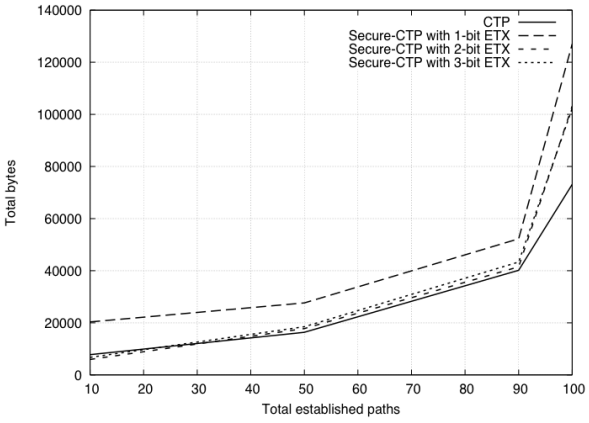


Fig. 7. Dependence of established paths on total data.

	CTP –	S-CTP 1-bit ETX	S-CTP 2-bit ETX	S-CTP 3-bit ETX
Total frames	42,901	32,226	32,335	32,392
Total collisions	55,352	45,027	39,075	42,870
Collision prob.	**0.568**	**0.582**	**0.547**	**0.569**

Tab. 1. Collision probability in the radio channel.

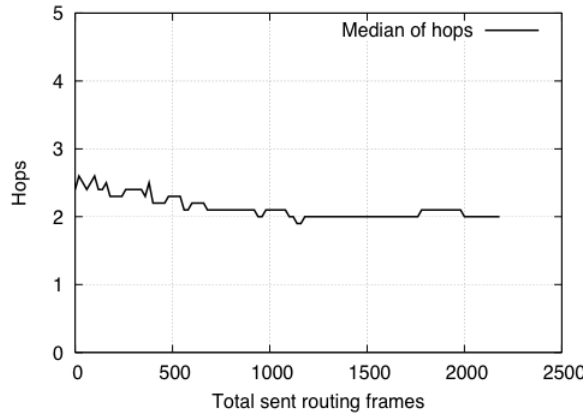
6.4 Routing Tree Convergence and Quality

Despite the efficiency and reliability of routing tree establishment, fast convergence of the paths belongs to the important characteristics of the routing protocols. For the next evaluation, we suppose that the network has the only suitable configuration of routing paths. If several possible trees are available, they have similar quality. In the calculations, median of ETX and median of hops are used as qualitative properties. Averaging of the medians was used for elimination of random biases.

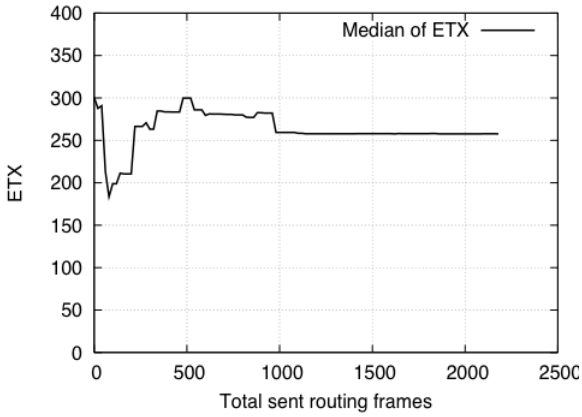
The evaluation was focused on alteration of routing paths quality in the amount of received routing frames. When 90 % of routing paths were established, the simulation starts. We were looking for the amount of data necessary for stabilizing the routing tree. The less routing frames are transmitted, the less energy is consumed by the routing protocol.

Graphical representations of the results (Figs. 8, 9, 10, 11) show that 1000 routing frames on average are necessary for stabilizing the routing tree. The results hold for the CTP and all variants of Secure-CTP. We have to mention the similarity of routing path quality of the CTP and the Secure-CTP with 1-bit ETX. Both protocols have converged to the same median of hops. This characteristic rises with the length of ETX. Thus we assume that the Secure-CTP with 1-bit ETX offers similar quality of the routing paths as the CTP.

The results cannot be compared by median of paths ETX as the CTP and Secure-CTP are based on a different distance function.

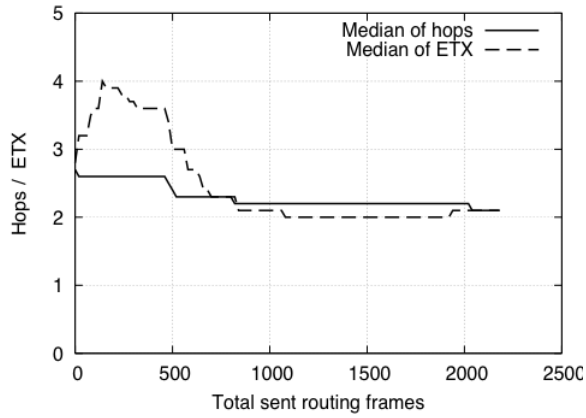


(a) Median of hops.

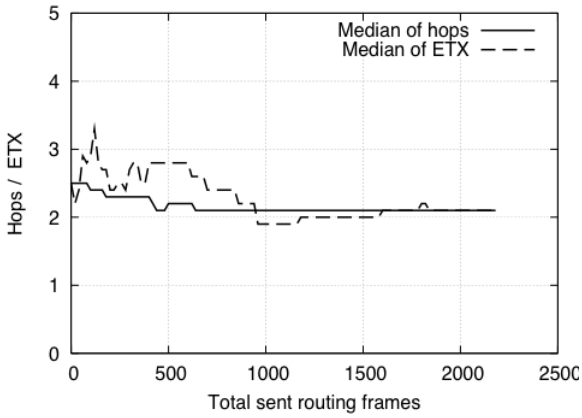


(b) Median of ETX.

Fig. 8. Routing tree convergence of the CTP.

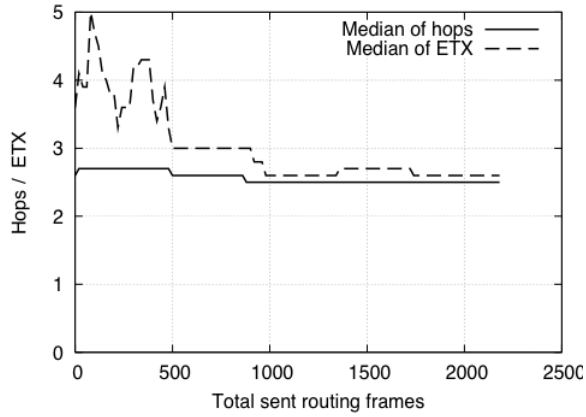


(a) Simulation 1.

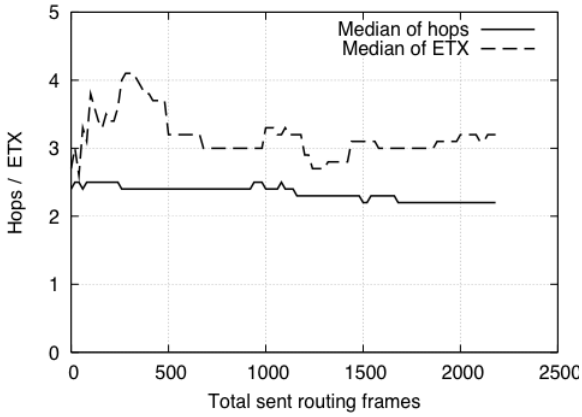


(b) Simulation 2.

Fig. 9. Routing tree convergence of the Secure-CTP with 1-bit ETX.



(a) Simulation 1.

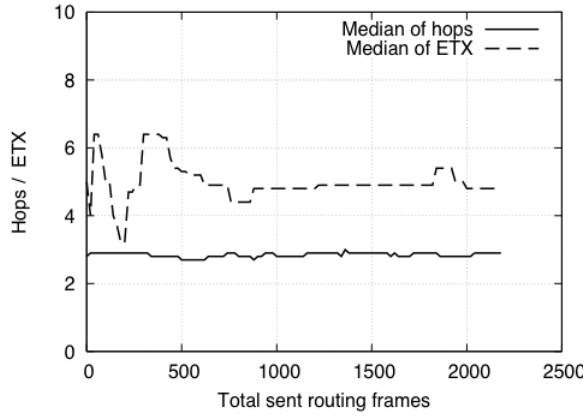


(b) Simulation 2.

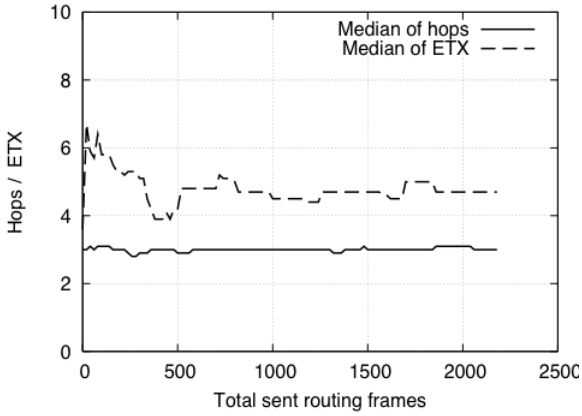
Fig. 10. Routing tree convergence of the Secure-CTP with 2-bit ETX.

Protocol	ETX	Sim.	Operation / Frame	10% depl. nodes		50% depl. nodes		90% depl. nodes		100% depl. nodes	
				Total frames		Total frames		Total frames		Total frames	
				Median	St.dev.	Median	St.dev.	Median	St.dev.	Median	St.dev.
CTP	–	1	recv(BF)	653	913	689	896	759	935	833	945
			send(BF)	91	96	97	96	105	99	110	100
			recv(RF)	9	4	323	176	1,531	521	3,288	847
			send(RF)	11	1	106	33	398	98	807	218
			Total bytes	**7,775**	**10,728**	**16,355**	**11,988**	**40,150**	**19,820**	**73,110**	**37,890**
CTP	–	2	recv(BF)	365	457	412	455	426	498	442	516
			send(BF)	58	53	63	53	65	57	65	58
			recv(RF)	12	2	447	187	1,680	233	3,025	503
			send(RF)	11	1	122	41	458	66	798	127
			Total bytes	**4,543**	**5,996**	**15,435**	**9,460**	**37,893**	**19,296**	**61,825**	**38,026**
Secure-CTP	1 bit	1	recv(BF)	1,777	1,065	1,868	1,079	2,059	1,149	2,081	1,154
			send(BF)	216	109	234	112	260	122	269	122
			recv(RF)	11	4	172	75	832	178	3,342	1,252
			send(RF)	11	1	82	17	309	39	1,176	415
			Total bytes	**20,438**	**14,227**	**27,644**	**15,505**	**52,234**	**25,146**	**126,973**	**74,481**
Secure-CTP	1 bit	2	recv(BF)	335	895	382	898	423	944	449	954
			send(BF)	65	96	70	98	77	106	81	108
			recv(RF)	10	3	265	89	995	192	2,177	1,100
			send(RF)	11	1	103	23	352	51	682	357
			Total bytes	**4,501**	**11,115**	**14,510**	**13,578**	**42,048**	**24,845**	**74,365**	**65,050**
Secure-CTP	2 bits	1	recv(BF)	472	581	573	584	621	635	652	637
			send(BF)	79	64	89	66	97	74	110	76
			recv(RF)	11	1	278	120	1,126	169	3,121	731
			send(RF)	10	1	107	23	364	27	1,114	246
			Total bytes	**5,931**	**7,619**	**17,794**	**10,423**	**41,486**	**23,071**	**103,164**	**64,365**
Secure-CTP	2 bits	2	recv(BF)	385	1,090	441	1,073	466	1,121	510	1,127
			send(BF)	68	118	73	115	83	125	89	129
			recv(RF)	10	1	280	135	962	146	3,612	1,225
			send(RF)	10	0	99	30	336	32	1,194	384
			Total bytes	**4,955**	**13,008**	**16,218**	**15,504**	**38,633**	**26,020**	**127,459**	**79,663**
Secure-CTP	3 bits	1	recv(BF)	545	1,011	565	989	578	1,041	584	1,045
			send(BF)	84	106	88	107	92	116	95	115
			recv(RF)	10	8	310	147	1,068	268	2,611	855
			send(RF)	11	2	101	32	351	62	927	299
			Total bytes	**6,745**	**11,865**	**18,504**	**15,088**	**43,331**	**24,334**	**102,329**	**57,128**
Secure-CTP	3 bits	2	recv(BF)	261	606	365	607	389	643	409	651
			send(BF)	62	71	76	73	79	78	86	80
			recv(RF)	13	4	347	157	939	217	3,071	872
			send(RF)	11	1	132	34	334	45	1,075	289
			Total bytes	**3,777**	**7,259**	**16,539**	**11,072**	**39,848**	**20,668**	**103,493**	**59,275**

Tab. 2. Statistics of radio transmission for establishment of routing paths.



(a) Simulation 1.



(b) Simulation 2.

Fig. 11. Routing tree convergence of the Secure-CTP with 3-bit ETX.

7. Conclusion

Our effort was to find the influence of modifications in the Secure-CTP with regard to the original protocol. We tried to prove that adding security into the protocols does not necessarily mean higher demands on data transfer and thus power consumption. Using the simulation of the CTP and three variants of Secure-CTP similar behavior of protocols in networks of 100 nodes was proved. During the establishment of routing path of up to the 90 % of nodes, the differencies in protocols' behaviour was irrelevant. A significant change comes while establishing the last 10 % of routing paths. However, this increase is evident also in the CTP. The expected rise of collisions in the radio communication wasn't proved. This is due to lower traffic in the networks, despite longer routing frames.

Finally, the convergence of the routing tree was compared. The results have shown that the CTP and Secure-CTP with 1-bit ETX offer similar characteristics of established routing paths. However, all the variants of Secure-CTP as well as the CTP need the same amount of routing frames. We believe that the communication overhead during establishment of the last paths in the network is only caused by longer frames.

In the paper we manifest that security in the protocols may be achieved with low cost. The CTP and Secure-CTP with 1-bit ETX offer the same result. We have to mention, however, that design of efficient routing protocols for large ad-hoc networks is difficult and it is not evident how the changes will affect the protocol behavior.

Acknowledgments

This research was supported by the Research Plan No. MSM, 0021630528 – Security-Oriented Research in Information Technology.

References

[1] LEVIS, P., LEE, N. *TOSSIM: A Simulator for TinyOS Networks*. 2003.

[2] FONSECA, R., GNAWALI, O., JAMIESON, K., KIM, S., LEVIS, P., WOO, A. *Collection Tree Protocol (CTP)*. TEP 123 Draft, 2006.

[3] STAJANO, F., CVRČEK, D., LEWIS, M. *Steel, cast iron and concrete: security engineering for real world wireless sensor networks*. In *Proceedings of Applied Cryptography and Network Security Conference ACNS*. Santa Fe (USA), 2008, p. 460-478.

[4] PLATON, E., SEI, Y. Security software engineering in wireless sensor networks. In *Progress in Informatics*. National Institute of Informatics, 2008.

[5] *TinyOS 2.0.2 Documentation*. [Online] Cited 2009-03-24. Available at: http://www.tinyos.net/tinyos-2.x/doc/

[6] PECHO, P., ZBOŘIL, F., JR., DRAHANSKıY, M., HANÁČEK, P. Agent platform for wireless sensor network with support for cryptographic protocols. *Journal of Universal Computer Science* (in press).

[7] PECHO, P. *Security of Wireless Sensor Networks*. PhD thesis. Brno: Brno University of Technology, 2009 (to be published).

[8] *FIPS 81: Operational modes of DES*. Federal Information Processing Standard (FIPS), Publication 81. Washington D.C.: National Bureau of Standards, U.S. Department of Commerce.

[9] BUONADONNA, P., HILL, J., CULLER, D. Active message communication for tiny networked sensors. In *20th Annual Joint Conference of the IEEE Computer and Communications Societies*. Anchorage (Alaska), 2001.

[10] Chipcon AS, Texas Instruments. *CC2420: 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver. Datasheet*. 2006.

About Authors...

Peter PECHO received the Ing. (M.Sc.) degree from the Brno University of Technology (BUT), Faculty of Information Technology (FIT) in 2006. Now, is working toward the PhD at the Dept. of Intelligent Systems, BUT. His research interests are focused on wireless sensor networks, smart cards, and security.

Petr HANÁČEK is an associate professor at the Faculty of Information Technology, Brno University of Technology. He concerns with information system security, risk analysis, applied cryptography, and electronic payment systems for more than ten years. He is an independent consultant in this area.

Jan NAGY received the Ing. (M.Sc.) degree from the Brno University of Technology (BUT), Faculty of Information Technology (FIT) in 2006. Now he is working toward the Ph.D. degree at the Dept. of Intelligent Systems at FIT BUT. He is a member of Brno University Security Laboratory. His research interests are focused on security in general, especially security in sensor networks, wireless networks, and social networks.