Efektywne protokoły bezpieczeństwa dla bezprzewodowych sieci sensorycznych

Zbigniew Kotulski, Paweł Szałachowski, Tomasz Ciszkowski
Politechnika Warszawska, Instytut Telekomunikacji

Bogdan Księżopolski, Damian Rusinek
UMC-S w Lublinie, Instytut Informatyki

Igor Dunajewski,
Uniwersytet Kazimierza Wielkiego w Bydgoszczy

Plan prezentacji

1. Optymalne rozmieszczanie czujników
2. Badania laboratoryjne. Czynniki komunikacyjne i wydajność WSN
3. Skalowalne bezpieczeństwo w sieciach sensorycznych
4. Bezpieczna komunikacja. Poufność i uwierzytelnienie pakietów
5. Uwierzytelnienie sensorów, Broadcast Encryption, adresowanie w WSN

1. Optymalne rozmieszczanie czujników

Prace na temat optymalnego rozmieszczania czujników pomiarowych do odczytu parametrów stanu konstrukcji w wybranych punktach.

Kryterium optymalności: najlepsza aproksymacja stanu w innych punktach, najdokładniejsza identyfikacja parametrów konstrukcji (np. stałych materiałowych).
(bez uwzględniania czynników komunikacyjnych)

Piotr Kazimierczyk, Zbigniew Kotulski, "O optymalnym rozstawianiu czujników", *Prace IPPT - IFTR Reports*, Vol.42/87, pp.1-123, (1987).

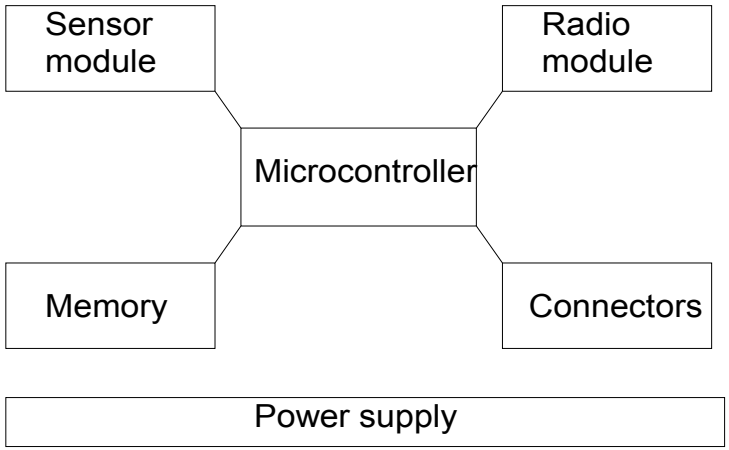
Piotr Kazimierczyk, “Optimal experiment design; Vibrating beam under random loading”, *European Journal of Mechanics. A. Solids*, Vol. 8, No.3, pp.161-184 (1989).

Zbigniew Kotulski, "Optimization of sensors' location in a stochastic extrapolation problem", *Journal of Sound and Vibration*, Vol.138, No.3, pp.351-363, (1990).

Reputacja jako miara optymalności

T.Ciszkowski, Z.Kotulski (2007). "Distributed Reputation Management in Collaborative Environment of Anonymous MANETs", *Proceedings of the IEEE International Conference on Computer as a Tool, EUROCON 2007*, pp. 1028-1033, (2007).

Tomasz Ciszkowski, Igor Dunajewski, Zbigniew Kotulski, "Reputation as optimality measure in Wireless Sensor Network-based monitoring systems", *Probabilistic Engineering Mechanics*, Vol.26, No.1, pp.67-75, (2011).



Pojawiły się Bezprzewodowe Sieci Sensoryczne (WSN) – z ich ograniczeniami

Teraz:

optymalizacja WSN =
optymalizacja sieci + optymalizacja pomiaru

Wspólną miarą optymalności może być **reputacja**

Zaufanie (*Trust*) i Reputacja (*Reputation*)

Zaufanie – prawdopodobieństwo, że uczestnik protokołu zachowa się zgodnie z oczekiwaniem (uczciwie).Można je obliczać (estymować). Jest subiektywne.

Reputacja – prawdopodobieństwo warunkowe uczciwego zachowania się uczestnika protokołu pod warunkiem znajomości jego (zakumulowanego) zachowania w przeszłości.

Dla sensorów:

Zaufanie: prawdopodobieństwo poprawnej transmisji pakietu

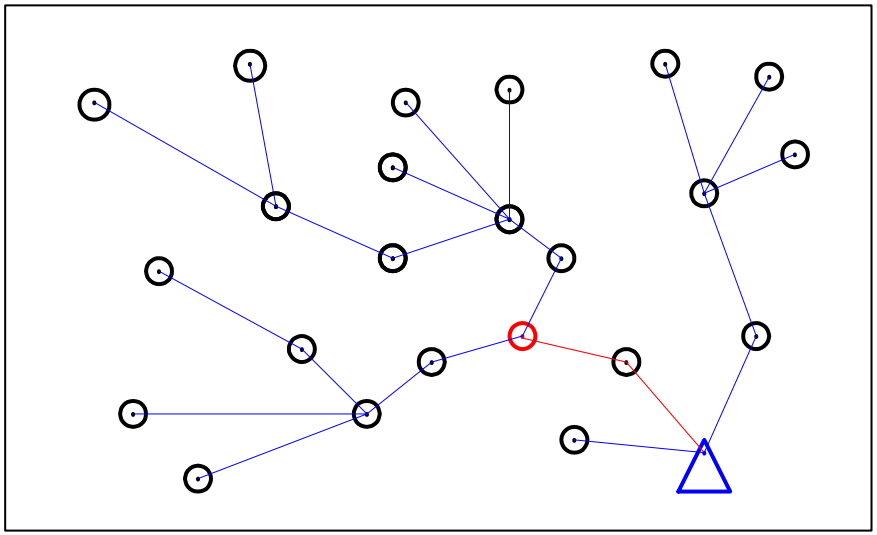
prawdopodobieństwo uzyskania wartościowego pomiaru

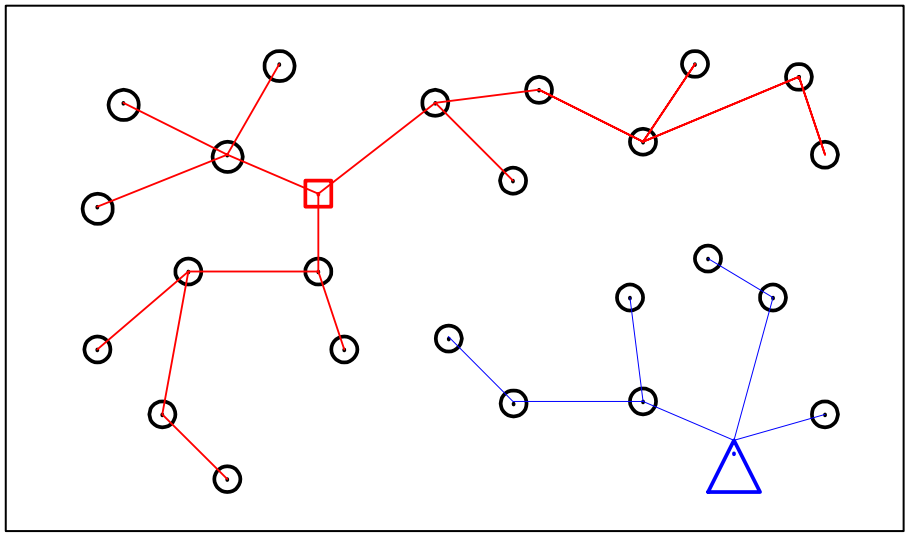
Reputacja: prawdopodobieństwo poprawnej transmisji pakietu określone na podstawie dłuższej obserwacji ścieżki

prawdopodobieństwo uzyskania wartościowego pomiaru określone na podstawie dłuższej obserwacji pomiarów

Routing w WSN

Znalezienie najlepszej ścieżki od sensora do stacji bazowej





Wyszukiwanie optymalnych ścieżek

Reputacja usługi (Service Reputation, SR)

- Odzwierciedla jakość transmisji

Zmienia się w czasie

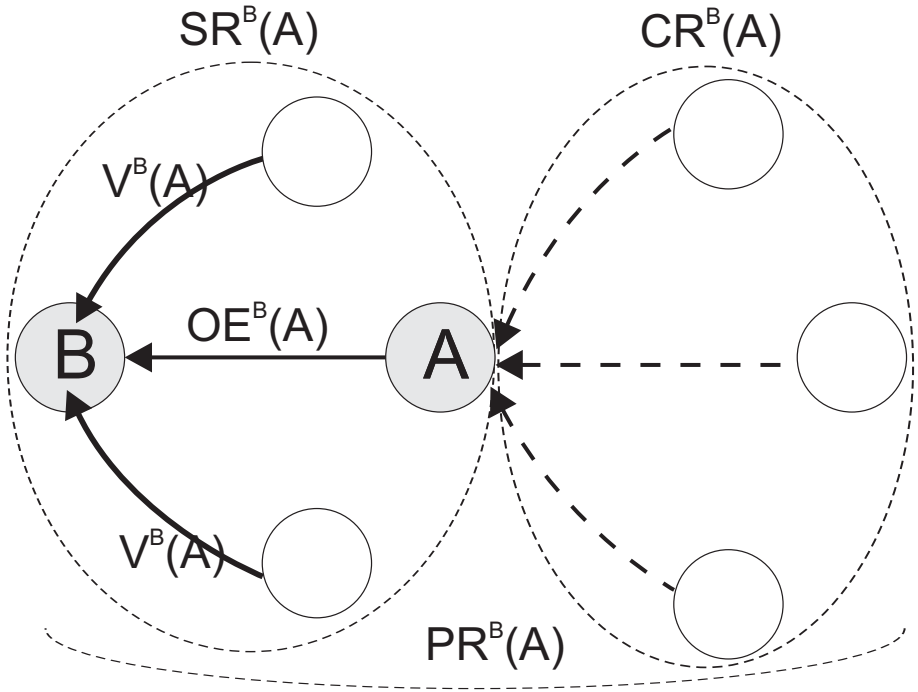
Jest obliczana na podstawie

- Własnych obserwacji (Own Experience, *OE*),
- Rekomendacji innych sensorów (Recommendations, *V*),
- Zaufania do węzła docelowego (End nodes' credibility, *IR*)

Każdy sensor pomiarowy inicjuje połączenie i znajduje ścieżkę do stacji bazowej

Wybiera ścieżkę o największej reputacji

Obserwacje sensora (węzła sieci P2P)



Own experience

Elementary Interactions STE and ***Satisfaction Degree ST***

$$STE_i^B(A) = \sum_{l=0}^{k-1} w_l P_l$$

$$ST_n^B(A) = \frac{1}{Q} \sum_{i=0}^{Q-1} STE_i$$

Obtained by neighborhood monitoring:

- packet modifications,
- delays,
- drops,
- errors.

Own experience based on finite history

Own experience ***OE*** of node *B* based on history of interactions with node *A*

$$OE_n^B(A) = \frac{\sum_{j=0}^{L-1} \gamma_j ST_{n-j}^B(A)}{\sum_{j=0}^{L-1} \gamma_j}$$

fading factor

$$\gamma_n = \begin{cases} \rho, & n = 0 \\ (1-\rho)^{n+1}, & n > 0 \end{cases} \quad 0 < \rho < 1$$

Reputation building

Service reputation ***SR*** of node A (based on own experience of B and experience of other voting nodes)

$$SR_n^B(A) = \alpha OE_n^B(A) + (1-\alpha)\frac{\sum_{p\in GVA} IR_n^B(p)V_n^p(A)}{\sum_{p\in GVA} IR_n^B(p)}$$

$$IR_n^B(p) > 0, \qquad 0 < \alpha < 1, \qquad \{B, C\} \subset GVA$$

Information reputation (credibility) $IR_n^B(C)$ of node C (based on own experience of B and experience of other voting nodes)

$$IR_n^B(C) = \beta OE_n^B(C) + (1-\beta)\frac{\sum_{p\in GIRSC} IR_n^B(p)\left|V_n^p(C) - OE_n^B(C)\right|}{2\sum_{p\in GIRSC} IR_n^B(p)}$$

$$IR_n^B(p) > 0, \qquad 0 < \beta < \alpha < 1, \qquad \{A, B\} \subset GIRSC$$

Reputation along the path

Cumulative reputation *CR* (the reputation of node A coming from nodes without direct connection to B)

$$CR_n^B(A) = IR_n^B(A)\frac{\sum_{p\in GA\setminus GB} V_n^p(A)}{|GA \setminus GB|}, \quad IR_n^B(A) > 0$$

Path reputation *PR* (own experience to first neighbor multiplied by cumulative reputation for the rest of the path)

$$PR_n^B(A) = SR_n^B(A)CR_n^B(A)$$

Samoorganizacja WSN

Każdy sensor wybiera własną ścieżkę do stacji bazowej

Sensory wysyłają pakiety z pomiarami

Niektóre sensory pośredniczące są przeciążone, więc ich reputacja maleje

Niektóre sensory znajdują nowe ścieżki (o wyższej reputacji)

Po kilku iteracjach wyboru ścieżek transmisja powinna się ustabilizować

Topologia ścieżek może się zmieniać w wyniku zmiany warunków zewnętrznych I zużycia baterii

Przy pewnych zmianach może powstać konieczność ponownego wyboru ścieżek

Optymalizacja sieci sensorów

W sieci bezprzewodowej aktywne sensory muszą zapewniać połączenie radiowe (stanowi to dodatkowy warunek przy optymalizacji sieci)

O akceptacji wyników pomiarów (przyjęcie lub odrzucenie danych do celów inżynierskich) można decydować również wykorzystując miarę analogiczną do reputacji (reputację pomiaru)

Reputacja pomiaru również może się zmieniać w czasie, więc sensory należy okresowo weryfikować (włączać lub wyłączać)

Cel: opracowanie inteligentnej metody wyboru sensorów konsolidującej obie miary reputacji

2. Badania laboratoryjne. Czynniki komunikacyjne i wydajność WSN

Igor Dunajewski, Zbigniew Kotulski, "Optimal wireless sensors' location for monitoring of structures in randomly disturbed environment", *PAMM*, Vol.9, No.1, pp.557-558, (2009).

Damian Rusinek, Bogdan Księżopolski, Zbigniew Kotulski, „Wpływ czynników komunikacyjnych na usługę dostępności w bezprzewodowych sieciach sensorycznych czasu rzeczywistego”, *Studia Informatica*, Vol.32, No.3A(98), pp.187-198, (2011).

Damian Rusinek, Bogdan Księżopolski, “Influence of CCM, CBC-MAC, CTR and Stand-Alone Encryption on the quality of transmitted data in the high-performance WSN based on Imote2”, *Annales UMCS Informatica AI XI*, 3, pp.117-127, (2011).

Sprzęt WSN

	IMOTE2	MICAz, MICA2	IRIS
			
Procesor	PXA271 Xscale (13/104/208/312/416 MHz)	Mikrokontroler Atmel Atmega128L	Mikrokontroler Atmel Atmega1281
Pamięć	256KB + 32MB	4KB + 512KB	4KB + 8KB
Radio	IEEE 802.15.4 2.4 GHz 250kbps	IEEE 802.15.4 2.4 GHz 250kbps	IEEE 802.15.4 2.4 GHz 250kbps
Pomiary	SHM-A Sensor Board, x-y-z, do 500 Hz	x-y, do 50 Hz	x-y, do 50 Hz

Systemy operacyjne: **LiteOS** i **TinyOS**

Pomiary: temperatura, naświetlenie, wilgotność i ciśnienie atm., przyspieszenie

Wpływ czynników zewnętrznych na transmisję w WSN (MICA2)

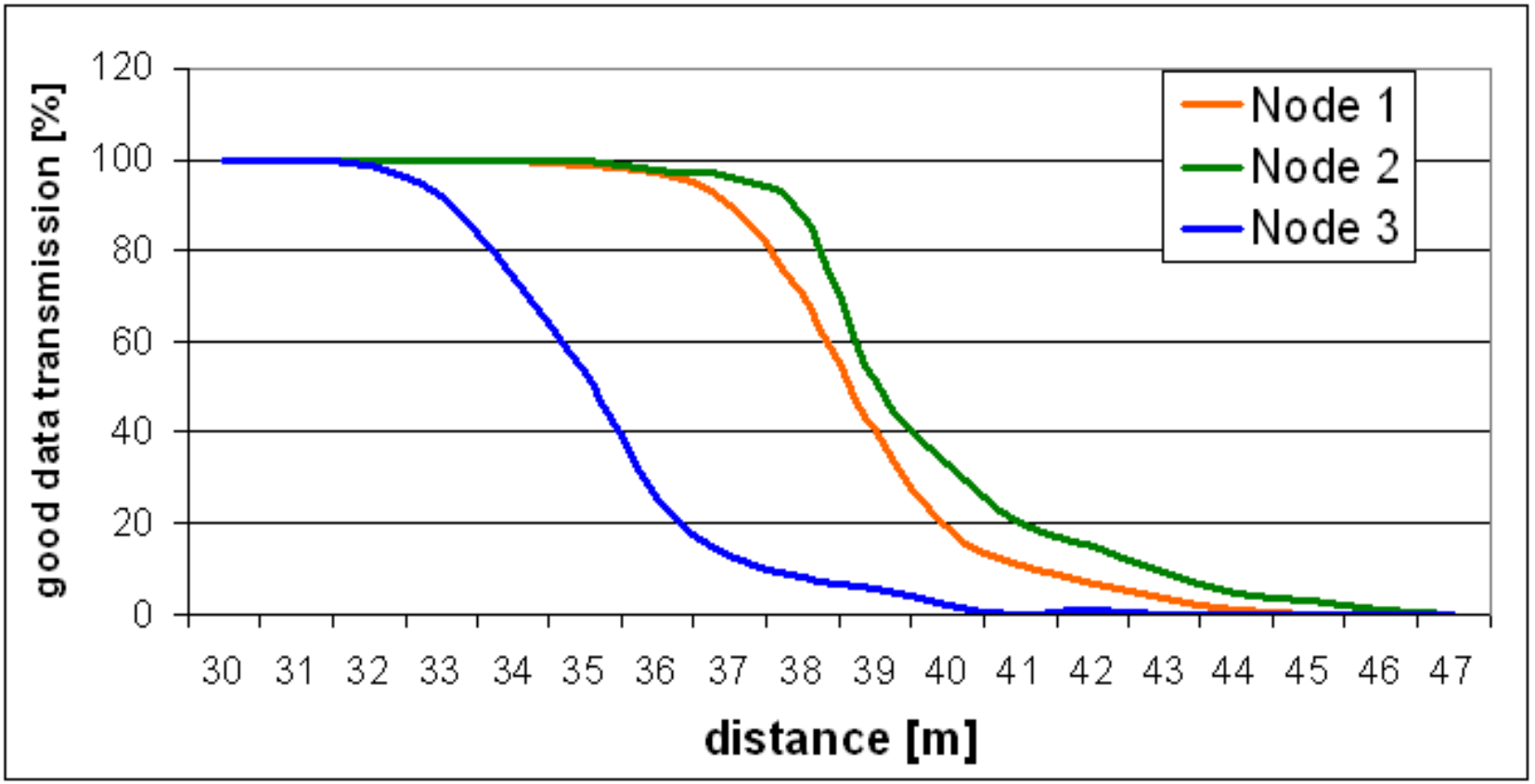
Jak zmieniają się własności sensorów w czasie działania ?

Jak różnią się własności komunikacyjne sensorów w zależności od czynników zewnętrznych i konfiguracji (topologii) sieci ?

Pomiary:

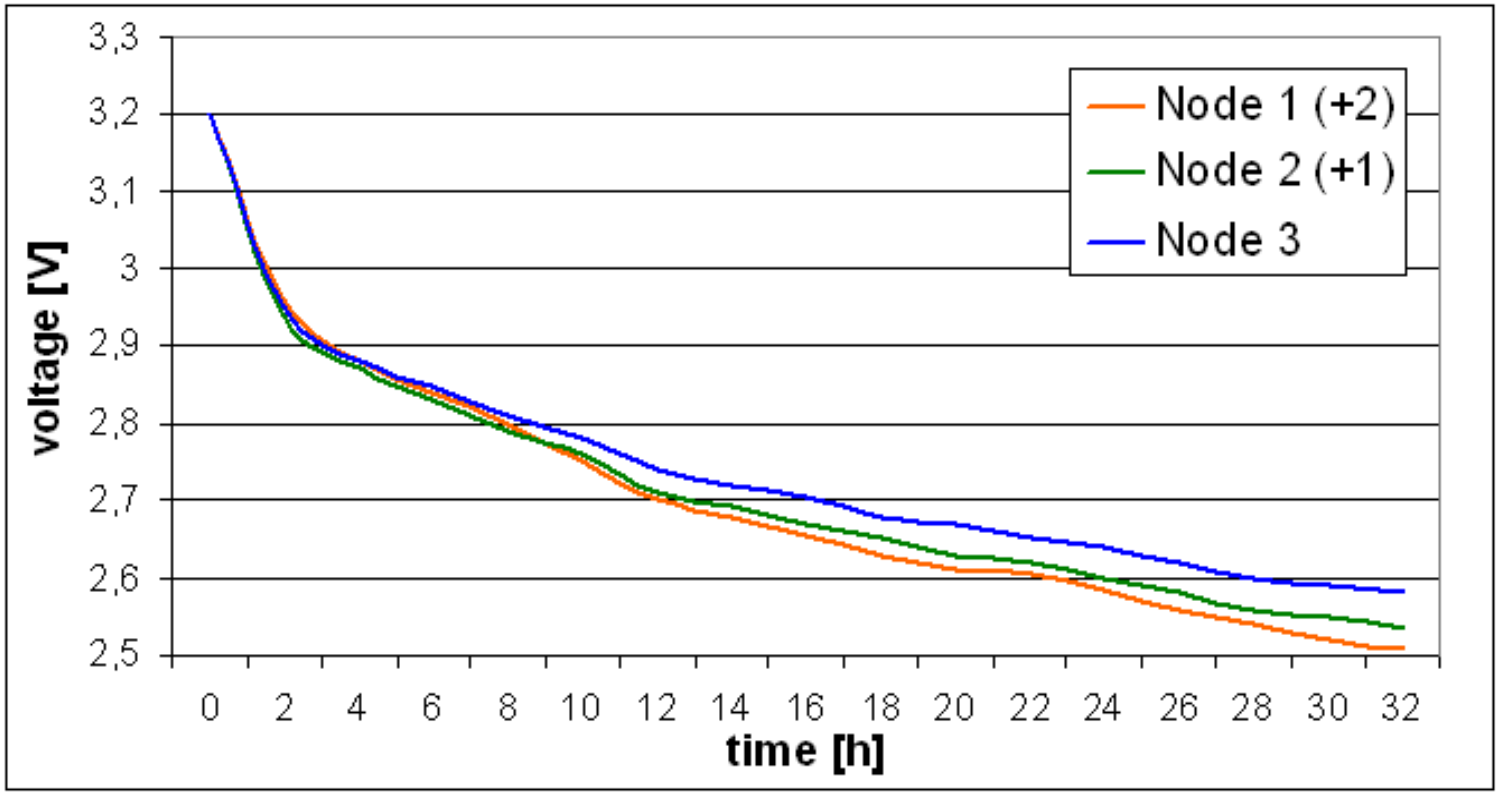
- Zasięg sensorów
- Jakość transmisji vs. poziom zaburzeń
- Czas działania sensorów
- Dokładność pomiaru vs. stan baterii

Zasięg sensorów

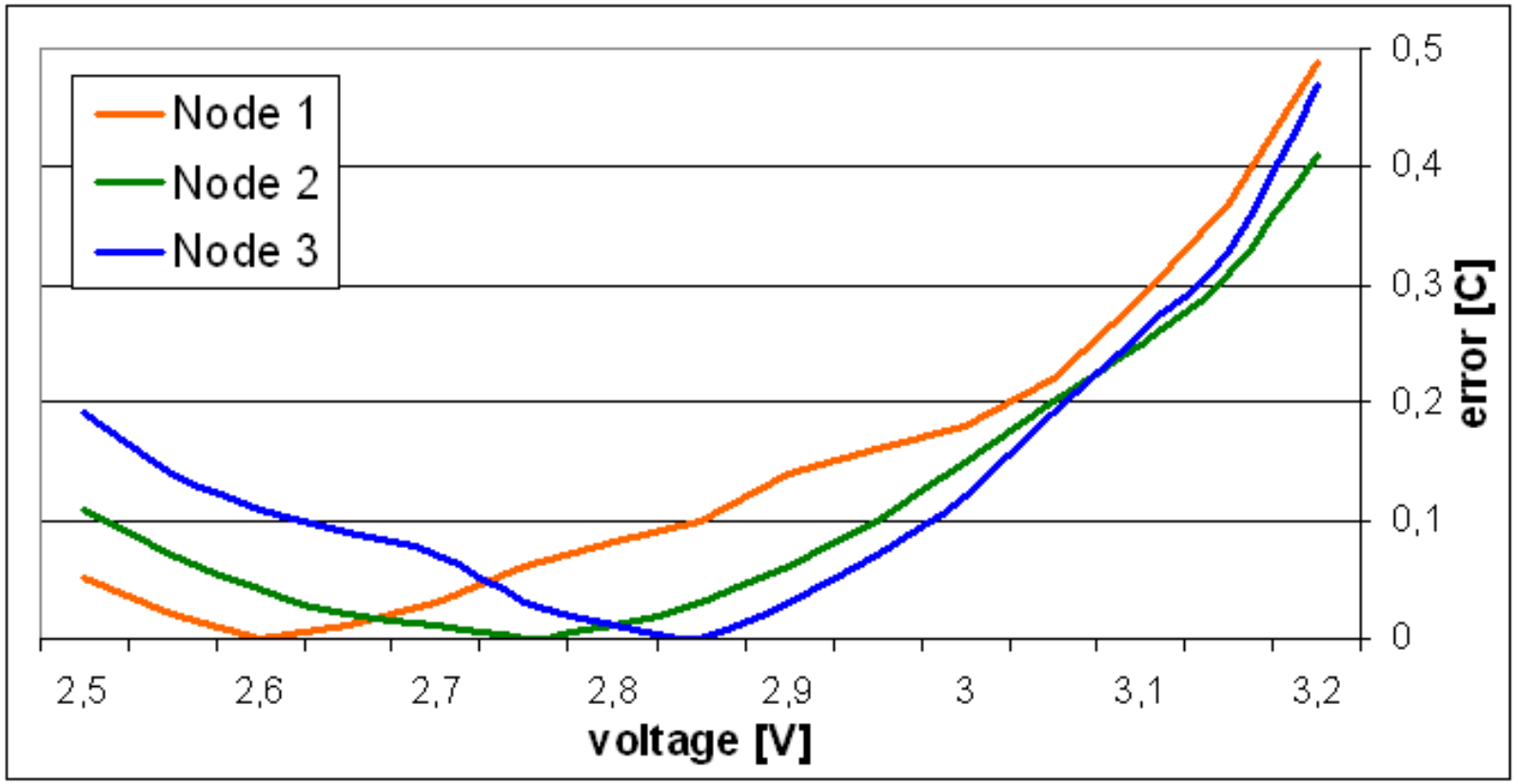


Jakość transmisji vs. poziom zaburzeń

Czas działania sensorów



Dokładność pomiaru vs. stan baterii



Badanie wpływu czynników komunikacyjnych na prędkość transmisji (IMOTE2)

Czynniki:

1. **Siła sygnału**

Manipulowanie mocą, z jaką wysyłany jest pakiet

2. **Rozmiar danych**

Manipulowanie rozmiarem wysyłanego pakietu

3. **Warstwa Łącza Pakietów (ang. PLL - Packet Linking Layer)**

Warstwa odpowiedzialna za retransmisję niepotwierdzonych pakietów

4. **Oszacowanie wolnego kanału (ang. CCA - Clear Channel Assessment)**

Jeśli kanał jest zajęty, radio odczekuje losowy kwant czasu

5. **Nasłuchiwanie przy niskiej mocy (ang. LPL - Low Power Listening)**

Celem tej funkcji jest wydłużenie pracy baterii. Sensor nie nasłuchuje ciągle czy nadchodzi pakiet, lecz asynchronicznie odpytuje radio

Rozmiar danych		Czas w ms								
		32B			64B			116B (max)		
Siła sygnału		5	15	25	5	15	25	5	15	25
CCA LPL PLL	Min	9,7	9,72	9,95	13,73	13,93	13,93	20,83	20,65	21,09
	Max	23,42	17,58	18,37	22,84	22,83	22,84	29,16	29,53	40,89
	Średnia	13,85	13,99	13,99	18,15	18,25	18,26	24,7	24,98	25,5
LPL PLL	Min	8,36	8,36	8,36	12,53	12,53	12,53	19,27	19,27	19,27
	Max	9,93	9,95	9,96	14,14	14,08	14,13	20,86	20,86	20,84
	Średnia	8,41	8,41	8,41	12,58	12,58	12,56	19,31	19,31	19,31
PLL	Min	8,03	8,03	8,03	12,16	12,16	12,16	18,89	18,89	18,89
	Max	20,75	20,75	20,75	26,82	26,84	26,82	35,72	36,1	36,1
	Średnia	8,17	8,17	8,17	12,33	12,33	12,33	19,18	19,28	19,08
Brak	Min	7,6	7,6	7,6	11,75	11,76	11,75	18,49	18,49	18,49
	Max	7,86	8,18	8,19	12,36	12,34	12,36	18,72	18,77	19,13
	Średnia	7,62	7,62	7,62	11,78	11,78	11,78	18,5	18,5	18,51

Tabela: Wpływ czynników na prędkość transmisji

Rozmiar danych = 116B	Czas w ms				
	Min	Max	Średnia	Moda (% wyst.)	Utracone pakiety (%)
Brak	18,49	19,13	18,51	18,49 (60%)	2,00%
LPL	18,77	21,33	18,83	18,81 (51%)	0,00%
PLL	18,89	36,1	19,09	18,92 (39%)	0,00%
CCA	19,9	28,78	24,19	24,96 (4%)	0,00%

Tabela: Wyniki testów LPL, PLL oraz CCA (rozmiar danych = 116B)

Rozmiar danych	Czas w ms				
	Min	Max	Średnia	Moda (% wyst.)	Utracone pakiety (%)
Domyślny (28B)	7,06	7,64	7,08	7,08 (52%)	2,00%
32B	7,6	7,86	7,62	7,61 (56%)	3,00%
64B	11,75	12,34	11,78	11,77 (52%)	2,00%
116B	18,49	19,13	18,51	18,49 (60%)	2,00%

Tabela: Test rozmiaru danych

Siła sygnału	Czas w ms				
	Min	Max	Średnia	Moda (% wyst.)	Utracone pakiety (%)
Domyślna (31)	7,05	7,64	7,08	7,08 (56%)	2,00%
5	7,05	7,64	7,08	7,08 (51%)	2,00%
15	7,05	7,64	7,08	7,08 (58%)	2,00%
25	7,06	7,64	7,08	7,08 (51%)	2,00%

Tabela: Test siły sygnału

Badanie wpływu trybów CCM, CBC-MAC, CTR oraz Stand-Alone Encryption na jakość transmisji (IMOTE2)

Szyfrowanie wykorzystujące tryby (AES 128).

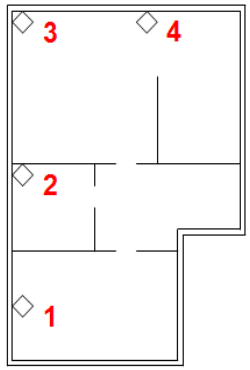
- Radio chip CC2420 umożliwia szyfrowanie wysyłanych pakietów poprzez ustawienie odpowiednich metadanych pakietu.
- Szyfrowanie można wykorzystać jedynie do szyfrowania wysyłanych pakietów.
- Szyfrowany jest cały pakiet: *header* + *payload*

Stand-Alone Encryption (AES 128).

- Szyfrowanie udostępnione przez chip CC2420, które może być wykorzystane nie tylko do szyfrowania ramek (wysyłanych pakietów).
- W badaniu szyfrowany jest tylko *payload*

Badana sieć

W badaniu zbudowano sieć składającą się z 4 sensorów IMOTE2. Badana była utrata pakietów (w procentach) na poszczególnych sensorach w zależności od interwału między kolejnymi próbkowaniami i ich przesyłaniem.



Interwał (ms)	250	200	150	100	75	50	25
Utrata pakietów (sensor nr 2) (%)	0	0	0	0	0	74,25	81,75
Utrata pakietów (sensor nr 3) (%)	0	0	0	0	0,5	3,75	44,75
Utrata pakietów (sensor nr 4) (%)	0	0	0	0,5	0	4	58,25
Średnia utrata pakietów (%)	0	0	0	0,17	0,17	27,33	61,58

Tabela: Niezabezpieczona sieć

Interwał (ms)	250	200	150	100	75	50	25
Utrata pakietów (sensor nr 2) (%)	0	0	0	0	1	68,25	59,75
Utrata pakietów (sensor nr 3) (%)	0	0,5	0,25	0,25	0	14,75	72,75
Utrata pakietów (sensor nr 4) (%)	0	0,25	0,75	0	0	5,05	43,75
Średnia utrata pakietów (%)	0	0,25	0,33	0,08	0,33	29,05	58,75

Tabela: Stand-Alone Encryption

Interwał (ms)	250	200	150	100	75	50	25
Utrata pakietów (sensor nr 2) (%)	0	0	0	0	12	78,25	89,75
Utrata pakietów (sensor nr 3) (%)	0,25	0	0	0	2,5	20,75	54,75
Utrata pakietów (sensor nr 4) (%)	0	0	0	0	2	9,75	57
Średnia utrata pakietów (%)	0,08	0	0	0	5,5	36,25	67,17

Tabela: CTR

Interwał (ms)	250	200	150	100	75	50	25
Utrata pakietów (sensor nr 2) (%)	0	0	0	0	38	76,5	90
Utrata pakietów (sensor nr 3) (%)	0	0	0	0	4,5	35,25	58,5
Utrata pakietów (sensor nr 4) (%)	0	0,75	0	0,25	2,5	15,75	58
Średnia utrata pakietów (%)	0	0,25	0	0,08	15	42,5	68,83

Tabela: CBC-MAC (16 bytes)

Interwał (ms)	250	200	150	100	75	50	25
Utrata pakietów (sensor nr 2) (%)	0	0	1,25	3,75	49,75	79,25	77,25
Utrata pakietów (sensor nr 3) (%)	0	0,25	0	3,5	8,5	13,75	76,25
Utrata pakietów (sensor nr 4) (%)	0	0	0	2,75	6,25	38,25	53,25
Średnia utrata pakietów (%)	0	0,08	0,42	3,33	21,5	43,75	68,92

Tabela: CCM (16 bytes)

3. Skalowalne bezpieczeństwo w sieciach sensorycznych

Bogdan Księżopolski, Zbigniew Kotulski, "On scalable security model for sensor networks protocols", In: R.J.Scherer, P.Katranuschkov, S.-E.Schapke [Eds.], *CIB-W78 2005, 22nd Conference Information Technology in Construction*, CIB Publication No.304, pp.463-469, Dresden 19-21 July 2005.

Bogdan Księżopolski, Zbigniew Kotulski, "Adaptable security mechanism for dynamic environments", *Computers & Security*, Vol.26, No.3, pp.246-255, (2007).

Bogdan Księżopolski, Zbigniew Kotulski, Paweł Szałachowski, "Adaptive Approach to Network Security", In: A. Kwiecień, P.Gaj, and P.Stera [Eds.], *CN 2009, Communications in Computer and Information Science*, Vol.39, pp.233-241, Springer-Verlag, Berlin Heidelberg 2009.

W WSN szczególnie istotne jest odejście od praktyki stosowania maksymalnych możliwych zabezpieczeń.

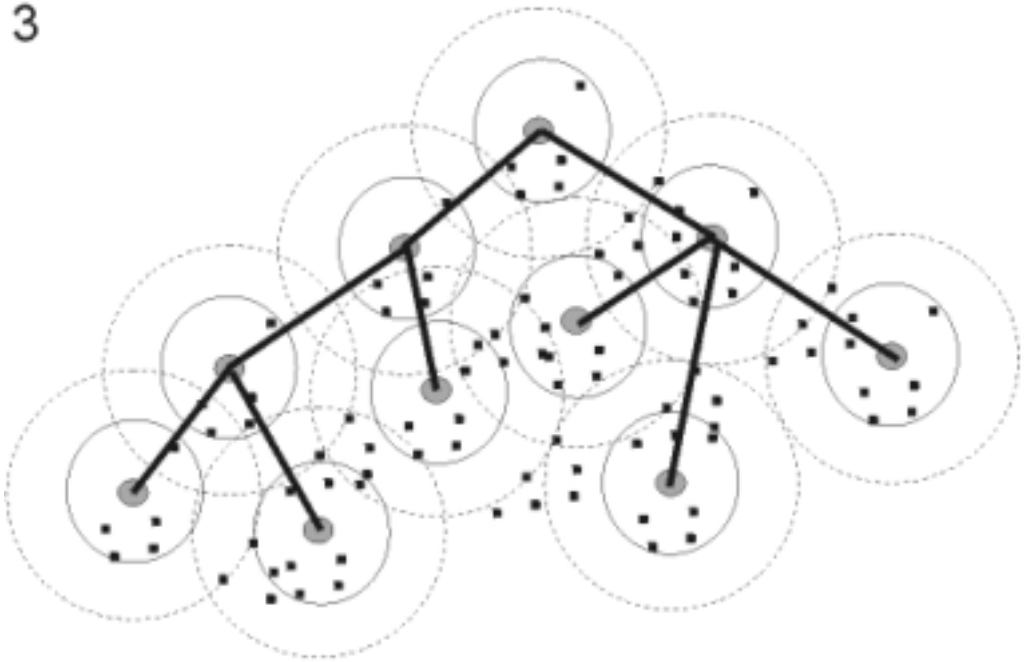
Należy poziom zabezpieczeń dostosowywać do warunków pracy sieci (obciążenie procesora, dopuszczalne opóźnienia, poziom baterii, poziom zaburzeń transmisji).

Hierarchiczna struktura sieci

Zakwalifikowanie sensorów do jednej z dwóch kategorii

głównych (wydajne sensory i łącza, silne zabezpieczenie)

dodatkowych (słabsze sensory, brak lub słabe zabezpieczenia)



Zastosowanie zróżnicowanych mechanizmów bezpieczeństwa

Dostosowanie poziomu zabezpieczeń sieci (węzłów) na podstawie analizy ryzyka

$$F_S = \frac{1}{a}\sum_{i=1}^{a}\frac{1}{b_i}\sum_{j=1}^{b_i}\frac{1}{c_{ij}}\sum_{x=1}^{c_{ij}}(L_{ij}^{x})^{Z}[(1-\omega_{ij}^{x})(1-P_{ij}^{x})];$$

i numer podprotokołu w protokole bezpieczeństwa,
j numer kroku w podprotokole,
x numer usługi bezpieczeństwa;
L_{ij}^{x} poziom zabezpieczeń usługi, $L_{ij}^{x} \in (0,1)$;
P_{ij}^{x} prawdopodobieństwo ataku na usługę, $P_{ij}^{x} \in (0,1)$;
Z współczynnik zbieżności, $Z \in (0,25)$
ω_{ij}^{x} średnia wartość strat w wyniku możliwego ataku, $\omega_{ij}^{x} \in (0,1)$;

Analiza protokołu SPINS zaproponowaną metodą

4. Bezpieczna komunikacja. Poufność i uwierzytelnienie pakietów

Paweł Szałachowski, Bogdan Księżopolski, Zbigniew Kotulski, "CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in wireless sensor networks", *Information Processing Letters*, Vol.110, No.7, pp.247-251, (2010).

Paweł Szałachowski, Bogdan Księżopolski, Zbigniew Kotulski, "On authentication method impact upon data sampling delay in Wireless Sensor Networks", In: A. Kwiecień, P.Gaj, and P.Stera [Eds.], *CN 2010, Communications in Computer and Information Science*, Vol.79, pp.280-289, Springer-Verlag, Berlin Heidelberg 2010.

Do zabezpieczenia komunikacji w WSN należy stosować algorytmy i protokoły dostosowane do możliwości sensorów

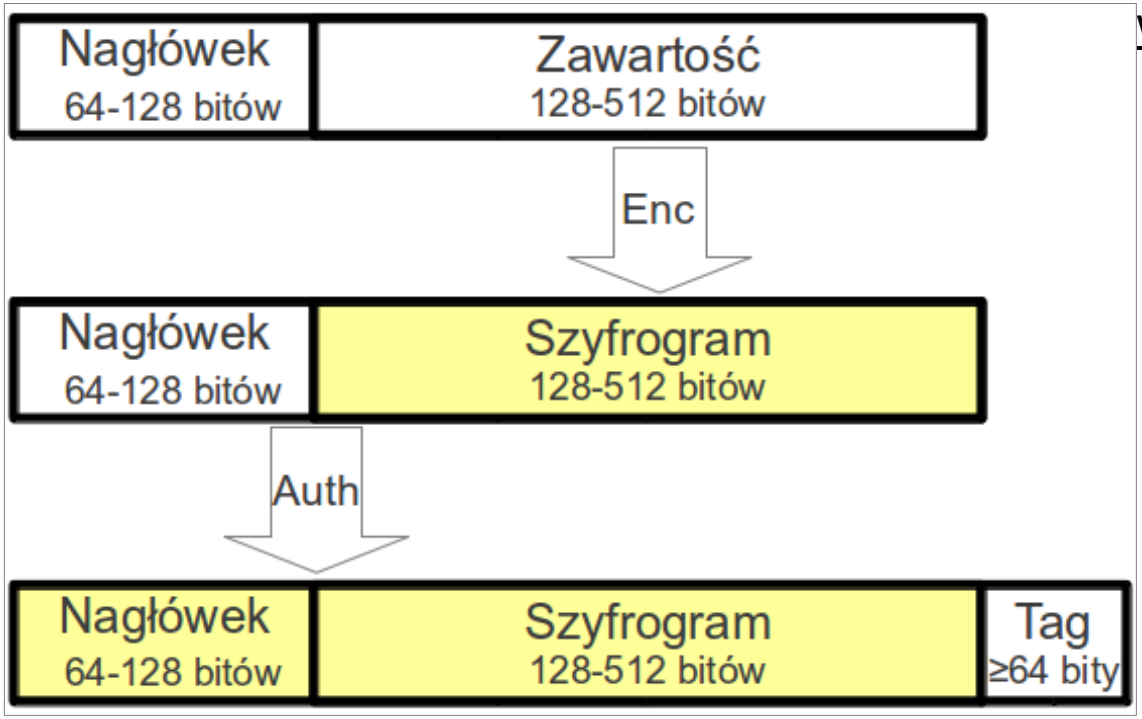
Takie metody można w znacznej części zaliczyć do lekkiej kryptografii

Bezpieczna komunikacja w WSN

Poufność jest usługą bezpieczeństwa gwarantującą, iż dane są dostępne jedynie dla uprawnionych podmiotów (np. realizowane jest za pomocą *szyfrowania*).

Uwierzytelnienie (również: *Autentyczność stron i pakietów*) jest usługą pozwalającą zweryfikować tożsamość podmiotów (np. stron komunikacji), jak i zidentyfikować pochodzenie danych (np. realizowane za pomocą *kodów MAC*).

Standardowe podejście:



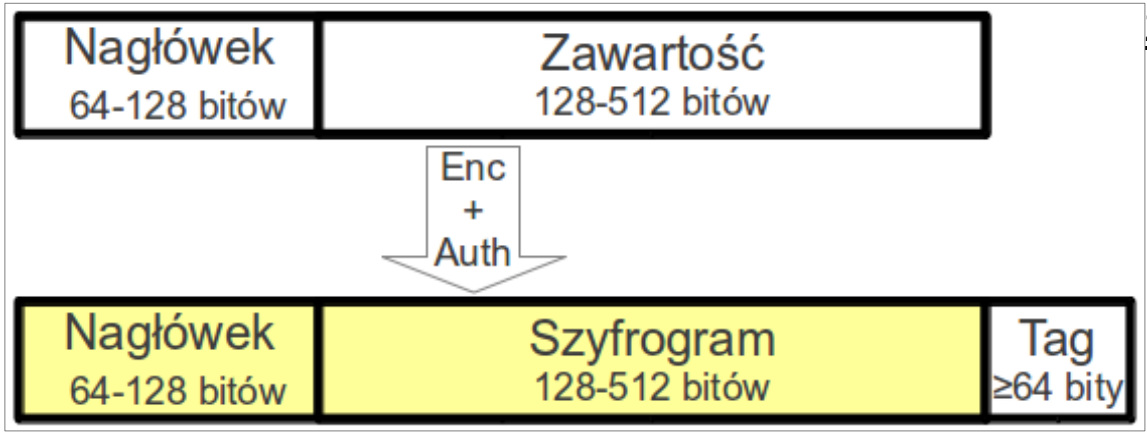
wady:

- zastosowanie dwóch operacji kryptograficznych
- przetwarzanie tych samych danych dwa razy
- wymagane dwa oddzielne klucze
- wymagane dwie implemetancje (szyfr+MAC)
- problemy z bezpieczeństwem (kolejność wykonywania operacji)

Tryb pracy szyfru blokowego: sposób, w jaki szyfr blokowy przetwarza dane w celu ich szyfrowania oraz deszyfrowania.

Zaawansowane tryby poza poufnością mogą zapewniać integralność/uwierzytelnianie – AEAD (*Authenticated Encryption with Associated Data*).

Wówczas operacja zabezpieczenia pakietu wygląda następująco:



zalety:

- jedna implementacja
- jeden klucz do szyfrowania oraz uwierzytelniania
- jednokrotne przetwarzanie danych

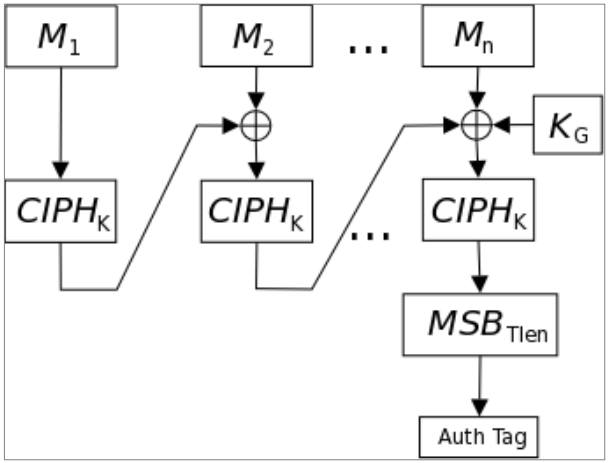
AEAD zapewnia dużą oszczędność obliczeniową oraz pamięciową, ale.

wymaga rozwiązania nowych problemów :

- jak skutecznie zrealizować schemat w WSN ?
- jak takie szyfrowanie zachowuje się dla bardzo krótkich wiadomości ?

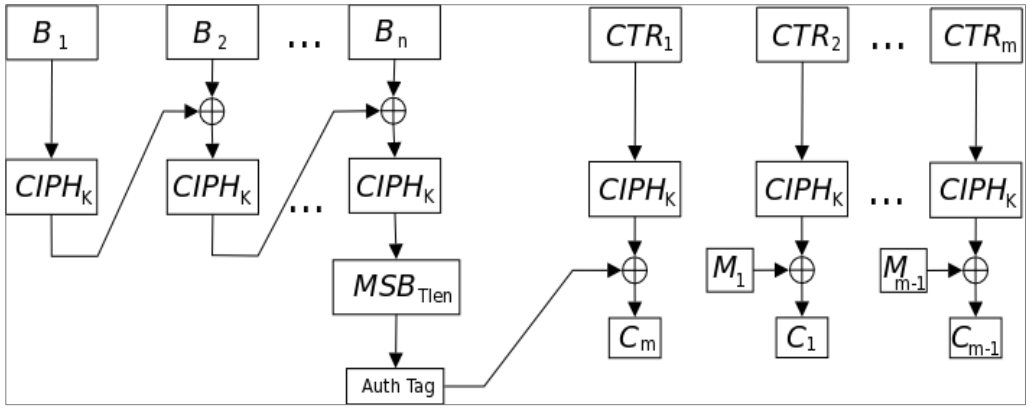
Tryb **CMAC** (*Cipher-based MAC*):

- prosta implementacja
- użycie funkcji szyfrowania do uwierzytelniania
- bardzo wydajny dla krótkich wiadomości
- posiada dowód bezpieczeństwa
- nie jest chroniony patentami
- standaryzowany

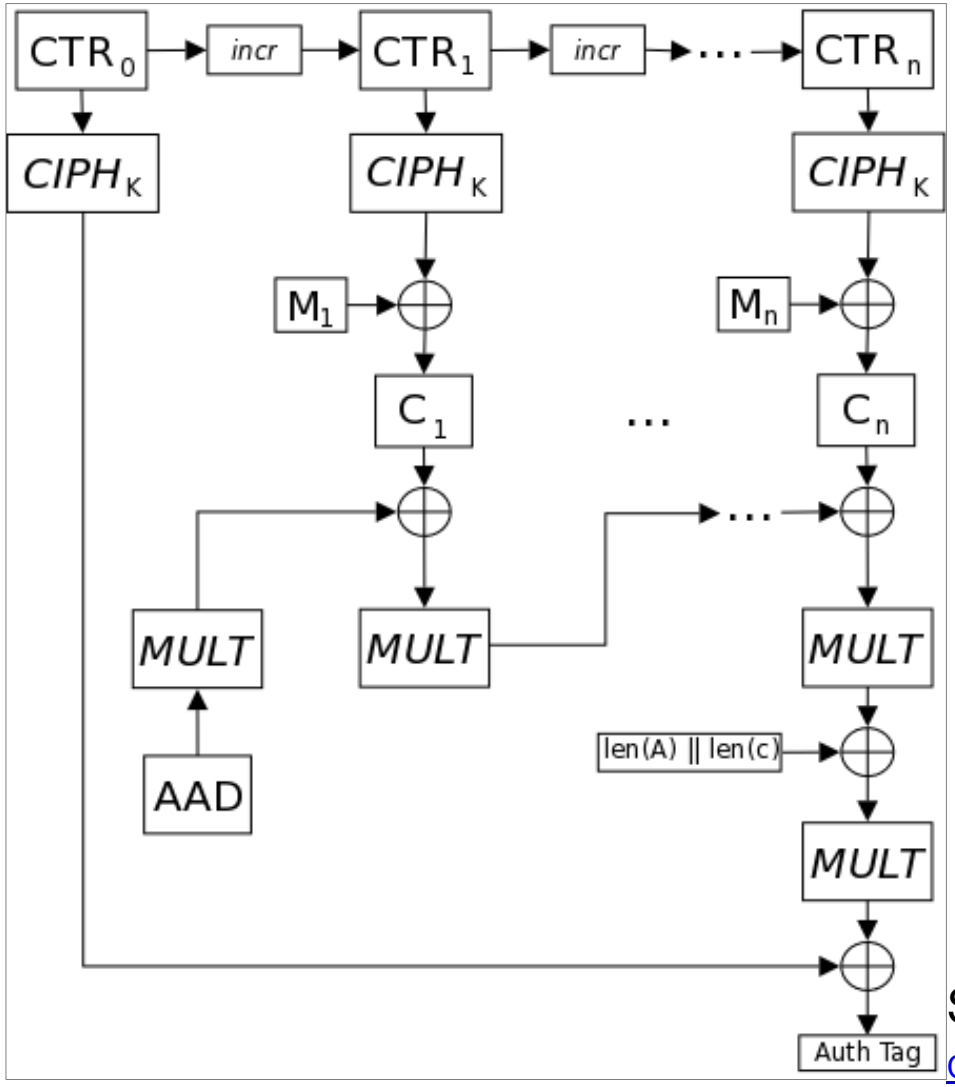


Tryb **CCM** (*Counter with CBC-MAC*):

- prosta implementacja
- wymaga jedynie funkcji szyfrowania szyfru blokowego
- szyfruje oraz uwierzytelnia dane
- posiada dowód bezpieczeństwa
- nie jest chroniony patentami
- standaryzowany



Tryb **GCM/GMAC** (*Galois/Counter Mode*):



- wymaga jedynie funkcji szyfrowania szyfru blokowego
- szyfruje oraz uwierzytelnia dane
- może jedynie uwierzytelniać (GMAC)
- uwierzytelnianie za pomocą działań w GF(2)
- łatwo zrealizować szybką implementację (sprzętową oraz programową)
- uwierzytelnenie przyrostowe (kolejny blok uwierzytelniany jest na podstawie swojej zawartości i aktualnego stanu)
- tryb bezpieczny (udowodniono)
- nie jest chroniony patentami
- standaryzowany

Szyfr **AES-128** (http://www.das-labor.org/wiki/AVR-Crypto-Lib/en)

XBow IRIS Mote (mikrokontroler ATmega1281, 8 KB RAM, 128 KB Flash)

Table 1
Performance of authenticated encryption modes.

Mode	Code size	Init	Size of AAD and payload (in bytes)											
			AAD	P	AAD	P	AAD	P	AAD	P	AAD	P	AAD	P
			8	16	8	32	8	64	16	16	16	32	16	64
CCM	4122 B	2597	658.79		560.15		489.63		592.50		532.39		479.98	
GCM	5706 B	21 085	984.50		842.22		747.37		736.28		700.45		671.80	
GCM-256B	6220 B	25 109	737.62		644.72		582.79		551.12		535.87		523.67	
GCM-4KB	10 271 B	57 686	500.62		455.12		424.79		373.37		377.87		381.47	
GCM-8KB	14 108 B	201 429	407.25		380.42		362.54		303.34		315.62		325.45	
EtM CMAC	3971 B	4211	505.70		438.87		401.44		466.46		423.93		396.13	

Table 2
Performance of authentication modes.

Mode	Code size	Init	Message size (in bytes)			
			16	32	48	64
CMAC	2240 B	5559	190.37	179.90	176.25	175.14
GMAC	5706 B	21 085	847.93	616.25	543.29	506.51
GMAC-256B	6220 B	25 109	601.06	431.09	378.79	352.21
GMAC-4KB	10 271 B	57 686	365.75	253.34	220.70	204.09
GMAC-8KB	14 108 B	201 429	270.68	183.31	158.45	145.73

Uwierzytelnienie (ECDSA jako przykład wydajnej kryptografii asymetrycznej):

Mode	Code size	Init	Message size (in bits)			
			128	256	384	512
CMAC	2240B	0.7ms	0.4ms	0.7ms	1.0ms	1.4ms
GMAC	5706B	2.6ms	1.7ms	2.5ms	3.2ms	4.0ms
GMAC-256B	6220B	3.1ms	1.2ms	1.7ms	2.3ms	2.8ms
GMAC-4KB	10271B	7.2ms	0.7ms	1.0ms	1.3ms	1.6ms
GMAC-8KB	14108B	25.1ms	0.5ms	0.7ms	0.9ms	1.2ms
HMAC-SHA1	5252B	0.0ms	4.7ms	4.7ms	4.8ms	4.8ms
HMAC-MD5	6348B	0.0ms	3.6ms	3.6ms	3.7ms	3.7ms
ECDSA sign	19308B	3493.4ms	2001.6ms	2001.6ms	2001.6ms	2001.6ms
ECDSA verify	19308B	3493ms	2436.5ms	2436.5ms	2436.5ms	2436.5ms

.

5. Uwierzytelnienie sensorów, Broadcast Encryption (BE), adresowanie w WSN

Paweł Szałachowski, Zbigniew Kotulski, Bogdan Księżopolski, "Secure position-based addressing scheme for WSN communication", In: A. Kwiecień, P. Gaj, and P. Stera [Eds.], *CN 2011, Communications in Computer and Information Science*, Vol.160, pp.386-397, Springer-Verlag, Berlin Heidelberg 2011.

Paweł Szałachowski, Zbigniew Kotulski, "Secure time information in the Internet Key Exchange Protocol", *Annales UMCS, Informatica*, Vol.AI 11, No.3, pp.41-56, (2011).

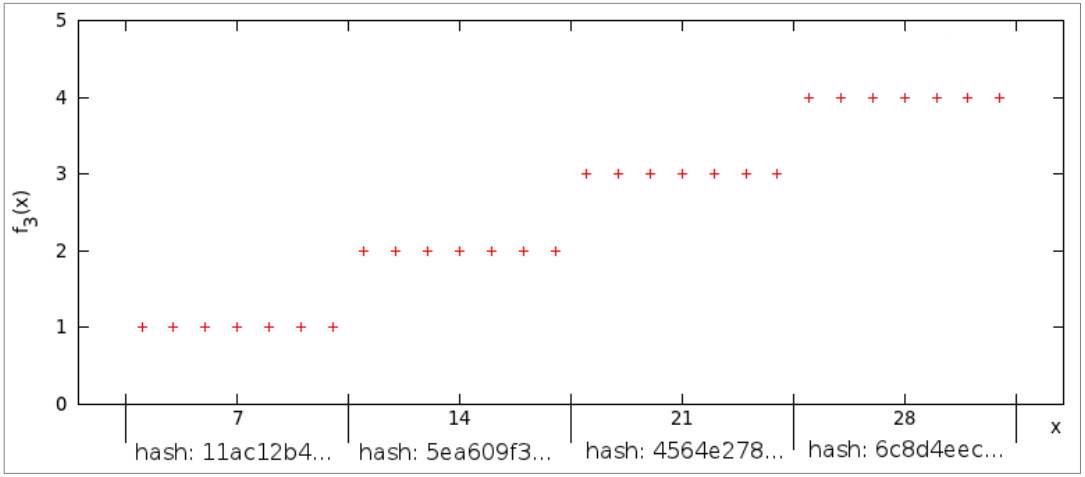
Zapewnienie, żeby dane docierały jedynie do uprawnionych węzłów

Zagwarantowanie poufności takiej transmisji

Problem adresowania wszystkich węzłów w danym obszarze

Wiadomość adresująca nie powinna zdradzać żądanego obszaru.
Adresowanie i weryfikacja powinny być szybkimi operacjami.

$$f_n(x) = \begin{cases} \frac{x}{p}, & r = 0 \\ \frac{x-r}{p}, & r \leq n \\ \frac{x+p-r}{p}, & r > n \end{cases}$$
where $p = 2n + 1$ and $r = x \mod p$.



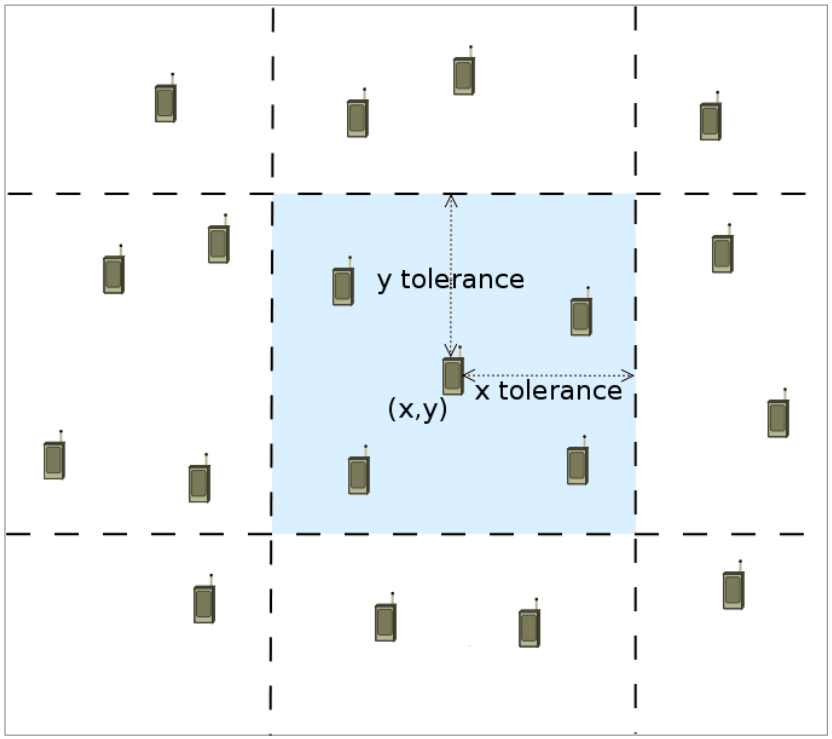
offset=x_R mod *p*
gdzie x_R jest wartością adresowaną

offset przekazywany jest wraz z wiadomością, ***n*** może być uzgodnione wcześniej

Zakładamy, iż każdy węzeł w sieci posiada tajny klucz ***K***

Wprowadźmy funkcję ***H***: {0,1}*→{0,1}^{a}, która jest jednokierunkowa i odporna na kolizje (tzn. jest obliczeniowo trudne znalezienie punktów x i x' takich, że x≠x' oraz H(x)=H(x')).

Przykład I adresacji dwuwymiarowej (prostokąt)



$$p_x = 2t_x + 1,$$

$$offset_x = x \mod p_x,$$

$$f_X = f(x - offset_x, t_x)$$

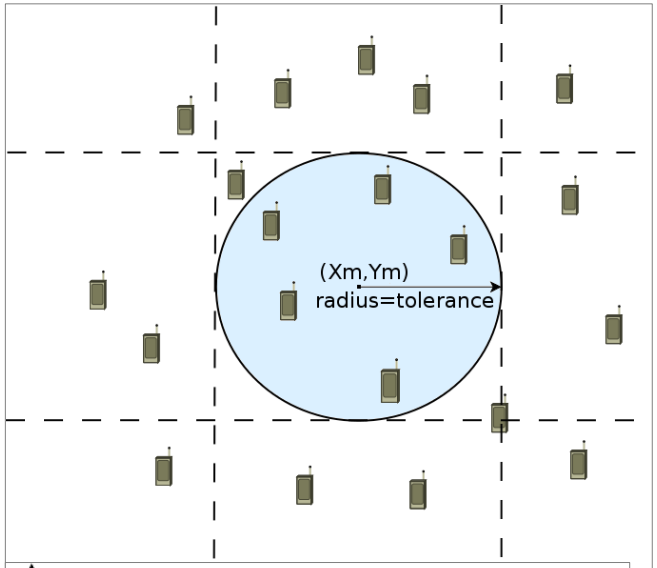
$$p_y = 2t_y + 1,$$

$$offset_y = y \mod p_y,$$

$$f_Y = f(y - offset_y, t_y)$$

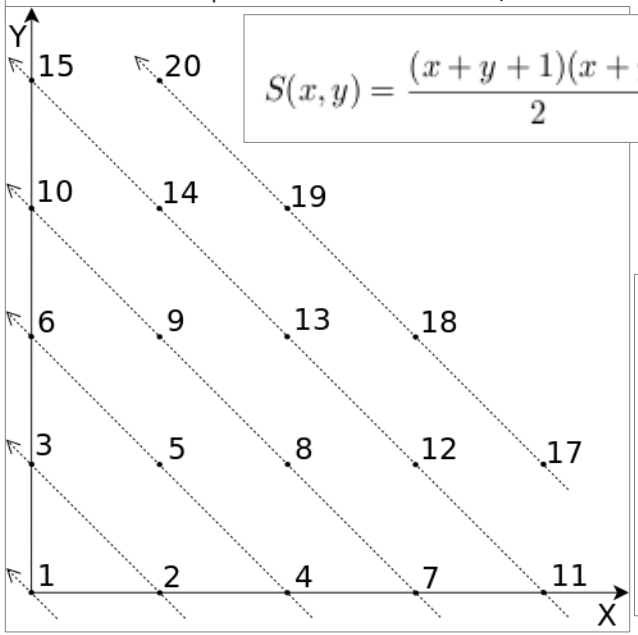
$$hash_{XY} = H(K \| t_x \| t_y \| offset_x \| offset_y \| f_X \| f_Y).$$

Przykład II



$$offset_x = x \mod p,$$
$$x_m = g(x - offset_x, radius)$$
$$offset_y = y \mod p,$$
$$y_m = g(y - offset_y, radius)$$

$$g(x,n) = \begin{cases} x, & r = 0 \\ x - r, & r \leq n \\ x + p - r, & r > n \end{cases},$$



$$S(x,y) = \frac{(x+y+1)(x+y)}{2} + y + 1$$

Adresowanie:

$$hash_s = H(K \| offset_x \| offset_y \| S(S(x_m, y_m), n))$$

Weryfikacja:

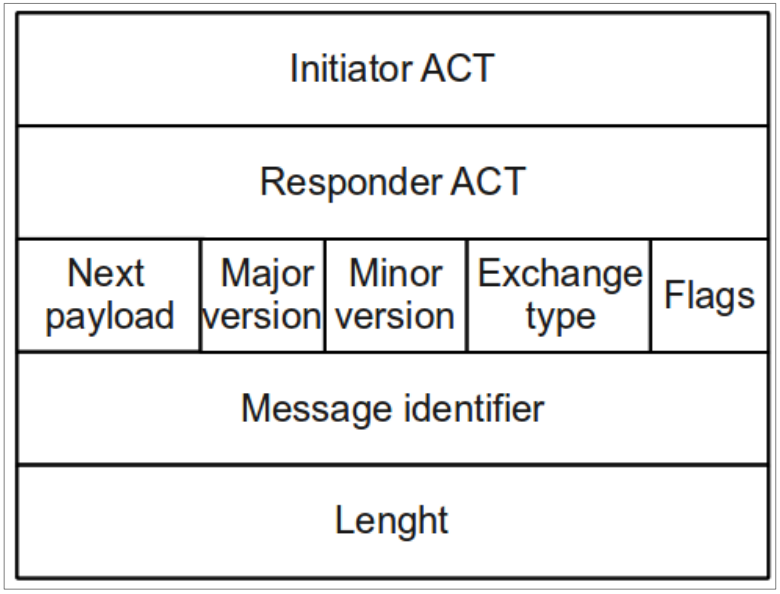
$$F(x, y, x_{mr}, y_{mr}, n) = \begin{cases} S(S(x_{mr}, y_{mr}), n), & (x - x_{mr})^2 + (y - y_{mr})^2 < n^2 \\ 0, & otherwise \end{cases}$$

$$hash = H(K \| offset_x \| offset_y \| F(x_r, y_r, x_{mr}, y_{mr}, n))$$

Inne zastosowanie konstrukcji

Bezpieczna synchronizacja czasu (gdy zegar jest rozsynchronizowany o najwyżej ***n*** jednostek)

Przykład: ISAKMP (*Internet Security Association and Key Management Protocol*)
Umieszczenie informacji w **A***nti*-**C***logging* **T***oken (ACT).*



Initiator:
send $(initmsg)$;

→

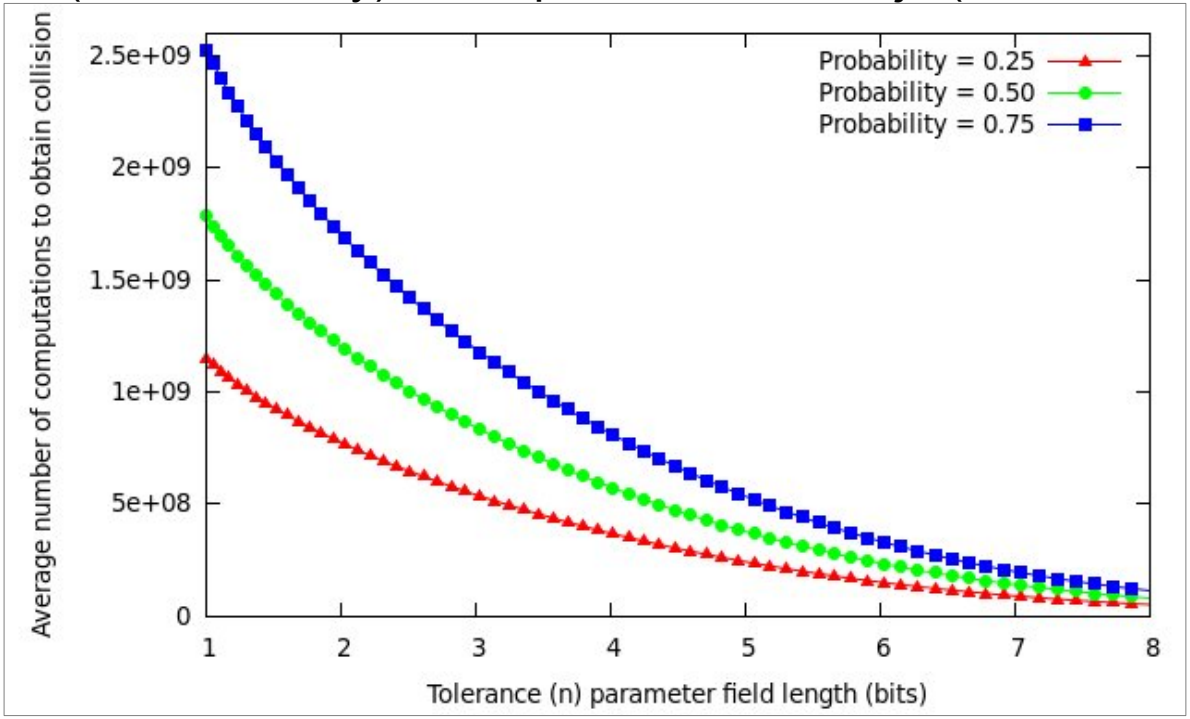
Responder:
t_R=get_time(); $\hat{o} = t_R \mod (2n+1)$;
$H_R = prf(K, IP_I \| IP_R \| P_I \| P_R \| n \| \hat{o} \| f_n(t_R - \hat{o}))$;
$ACT\text{-}R = H_R \| n \| \hat{o}$;
send $(ACT\text{-}R)$;

←

Initiator:
parse $(ACT\text{-}R)$; t_I=get_time();
$H_I = prf(K, IP_I \| IP_R \| P_I \| P_R \| n \| \hat{o} \| f_n(t_I - \hat{o}))$;
if H_I is equal H_R;
  adjust time by $\hat{o}$;
else
  need to synchronize

Analiza

Wymagana jedynie jedna (krótka) wiadomość i jedna operacja kryptograficzna.
Zbyt krótkie pole (ACT = 64 bity) może powodować kolizje (atak urodzinowy).



Nawet gdy klucz ***K*** zostanie skompromitowany, atakujący musi dokonać ataku przeszukiwania. Prawdopodobieństwo jego sukcesu wynosi:

$$\frac{q(2n+1)s}{2^k}$$

q – liczba obliczeń wykonanych przez atakującego
s – liczba podsłuchanych wiadomości
k – rozdzielczość (czasu/pozycji) w bitach

Przyszłe prace

Projekt

Energy-Aware Key Management in Mobile Wireless Sensor Networks

E-Key-Nets

7FP NoE Euro-NF Specific Joint Research Project

Partnerzy projektu:

Universität Passau, Niemcy

Research Centre of the Athens University of Economics and Business, Grecja

Politechnika Warszawska, Polska